
JRC TECHNICAL REPORTS

# Biometric Spoofing:
# A JRC Case Study in 3D Face Recognition

Javier Galbally
Riccardo Satta
Monica Gemo
Laurent Beslay

2014

Report EUR 27053 EN

Joint
Research
Centre

European Commission

Joint Research Centre

Institute for the Protection and Security of the Citizen

Contact information

Laurent Beslay

Address: Joint Research Centre, Via Enrico Fermi 2749, TP 361, 21027 Ispra (VA), Italy

E-mail: Laurent.beslay@jrc.ec.europa.eu

Tel.: +39-0332-786556

http://www.jrc.ec.europa.eu/



JRC 94041

EUR 27053 EN

ISBN 978-92-79-45024-2 (pdf)

ISSN 1831-9424

doi: 10.2788/00790

Luxembourg: Publications Office of the European Union, 20xx



Abstract:

Based on newly available and affordable off-the-shelf 3D sensing, processing and printing technologies, the JRC has conducted a comprehensive study on the feasibility of spoofing 3D and 2.5D face recognition systems with low-cost self-manufactured models and presents in this report a systematic and rigorous evaluation of the real risk posed by such attacking approach which has been complemented by a test campaign. The work accomplished and presented in this report, covers theories, methodologies, state of the art techniques, evaluation databases and also aims at providing an outlook into the future of this extremely active field of research.

# Table of Contents

# 1. Introduction

Launched in January 2014, the JRC institutional project 566-BBM (Biometric and Border Management) aims at providing a scientific support to the roll-out and improvement of biometrics in large-scale ID systems such as those used in border management (i.e. VIS, SIS2, EURODAC) as well as new generation of Automatic Border Control systems . The introduction of such systems still presents important technical challenges with regards to quality, security and privacy issues, which are addressed through the JRC BBM project by the development of tailored evaluation platform, reference methods and test protocols.

In the case of the deliverable of the project BBM which is presented in this report, the objective is to consolidate and develop test protocols for systematic spoof resistance testing for fingerprint, iris and face as well as preparatory activity for possible standardisation. Eventually the project intends foster through its scientific activities the main principles of the Charter of Fundamental Rights of the EU[1].

In recent decades, we have witnessed the evolution of the biometric technology from the first pioneering works in face and voice recognition to the current state of development where a wide spectrum of highly accurate systems may be found, ranging from largely deployed modalities like fingerprint, face or iris, to more marginal ones like signature or hand. This path of technological evolution has naturally led to a critical issue that has only started to be addressed recently: the resistance of this rapidly emerging technology to external attacks and, in particular, to *spoofing*.

Spoofing, strictly referred to with the term *presentation attack* in the current standards, is a purely-biometric vulnerability, not shared with other IT security solutions. It refers to the ability to fool a biometric system into recognizing an illegitimate user as the genuine one, by means of presenting to the sensor a synthetic forged version of the original biometric trait. The whole biometric community, including researchers, developers, standardizing bodies and vendors, has thrown itself into the very challenging task of proposing and developing efficient protection methods against this threat.

Based on newly available and affordable off-the-shelf 3D sensing, processing and printing technologies, the JRC has conducted a comprehensive study on the feasibility of spoofing 3D and 2.5D face recognition systems with low-cost self-manufactured models and presents in this report a systematic and rigorous evaluation of the real risk posed by such attacking approach which has been complemented by a test campaign. The work accomplished and presented in this report, covers theories, methodologies, state of the art techniques, evaluation databases and also aims at providing an outlook into the future of this extremely active field of research.

Several reasons have driven us to select the face biometric as the focal point of the present spoofing case study:

- According to the International Biometric Group (IBG), face is the second most largely deployed biometric at world level in terms of market quota right after fingerprint.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

- It is also adopted in most official identification documents such as the ICAO-compliant biometric passport or national ID cards. As such, nowadays face is one of the biometric traits with the highest potential impact both from an economic and a social point of view.
- Together with the fingerprint trait, it is most probably the biometric where the most spoofing-related research has been conducted, leading to a very large amount of published works. However, unlike in the fingerprint case, there is still no rigorous and comprehensive survey covering all the anti-spoofing methods proposed in the field of face recognition.

This JRC Technical Report is an attempt to contribute to this difficult review task as well as presenting a new spoofing research work in 3D face spoofing. It provides an overall picture of the current panorama in biometric spoofing with special focus on the face trait, the strengths, shortcomings and challenges of these security protection techniques. In addition, the report illustrates those challenges by presenting the results of a JRC spoofing test campaign on 3D face system supported by a low cost attack. The rest of the report is divided in three main sections:

- **Section 2. Introduction to spoofing**. This section concludes with an outline of the lessons learnt in these more than 10 years of intensive anti-spoofing research and with a proposed vision of the challenges to be faced and possible future JRC research lines that may contribute to the general improvement of the security level offered by biometric systems against spoofing.
- **Section 3. JRC case study in 3D face recognition spoofing**. Following a comprehensive survey of the spoofing and anti-spoofing methodologies proposed so far in the widely used face modality, this part presents the 3D face dataset developed by the JRC and the Test campaign applied to this test. It also provides an overview of the publicly available evaluation benchmarks for face anti-spoofing approaches, summarizing the detection rates achieved by state of the art methods in the international competitions that have been organized up to date.
- **Section 4. Summary and discussion: lessons, facts and challenges**.

# 2. Biometric Spoofing

## 2.1. Introduction

"Fingerprints cannot lie, but liars can make fingerprints". Unfortunately, this paraphrase of an old quote attributed to Mark Twain[2] has been proven right in many occasions now. And not only for fingerprints, but also for many other biometric traits such as face, iris, voice or even gait.

Every technology has its own time. Since the first pioneering works on automatic voice and face recognition over 40 years ago [1], [2], [3], steady and continuous progress has been made in the development of the biometric technology. Driven by the very appealing new security biometric paradigm "forget about cards and passwords, you are your own key", researchers from many different fields such as image processing, computer vision or pattern recognition, have applied the newest techniques in each of these areas to improve the performance of biometric systems [4]. This path of technological evolution has permitted the use of biometrics in many diverse activities such as forensics, border and access control, surveillance or on-line commerce.

In this scenario of constant expansion, and as a consequence of its own natural progress, new concerns are arising regarding the biometric technology different from the mere improvement of its recognition performance. Among these new issues and challenges that have emerged around biometrics, its resilience against external threats has lately drawn a significant level of attention.

Currently it is an accepted fact that, as the deployment of biometric systems keeps growing year after year in such different environments as airports, laptops or mobile phones, people are also becoming more familiar with their use in everyday life and, as a result, their security weaknesses are better known to the general public. Nowadays, it is not difficult to find websites or even tutorial videos, which give detailed guidance on how to create fake masks, fingerprints or irises that may be used to fool biometric systems.

Attacks are not any more restricted to a mere theoretical or academic sphere, but are starting to be carried out against real operational applications. The fairly easy hacking of the long anticipated new iPhone 5S fingerprint reader, just a day after it hit the shelves and using a regular and well-known type of fingerprint spoof [5], is only another example in the list of practical attacks and vulnerabilities of biometric systems that are being reported to the public from hacking groups attempting to get recognition [6], [7], [8], [9], [10], from real criminal cases [11], [12], [13], [14], or even from live demonstrations at biometric and security specific conferences [15], [16].

As a consequence, in recent years, there has been an increasing interest on the evaluation of biometric systems security, which has led to the creation of numerous and very diverse initiatives focused on this field of research [17], [18]: the publication of many research works disclosing and evaluating different biometric vulnerabilities [19], [20], [21], [22], [23], [24]; the proposal of new protection methods [25], [26], [27], [28]; related books and book chapters [29], [30], [31]; PhD and MSc Theses which propose and analyse different biometric spoofing and anti-spoofing techniques [32], [33], [34], [35], [36], [37], [38], [39]; the publication of several standards in the area [40], [41], [42] and of different Supporting Documents and Protection Profiles in the framework of the security evaluation standard Common Criteria for the objective assessment of commercial systems [43], [44];

[2] Figures do not lie, but liars do figure.

the certification of different commercial products in the framework of the Common Criteria [45], [46]; patented anti-spoofing mechanisms for biometric systems [48], [49], [50]; the dedication of specific tracks, sessions and workshops in biometric-specific and general signal processing conferences [51], [52], [53]; the organization of competitions focused on vulnerability assessment [54], [55], [56], the acquisition of specific datasets [57], [58], [59]; the creation of groups and laboratories specialized in the evaluation of biometric security [60], [61], [62]; or the existence of several European Projects with the biometric security topic as their main research interest [63], [64].

All these initiatives clearly highlight the importance given by all parties involved in the development of biometrics (i.e., researchers, developers and industry) to the improvement of the systems' security in order to bring this technology to comparable deployment levels to other well established security-related solutions.

Among the different vulnerabilities analyzed, intensive research efforts have been focused on the study of direct or spoofing attacks. Spoofing is a purely-biometric vulnerability, not shared with other IT security solutions. In these attacks, intruders use some type of synthetically produced artefact (e.g., face mask, gummy finger or printed iris image), or try to mimic the behaviour of genuine users (e.g., gait, signature), to fraudulently access the biometric system. In this way, spoofing takes advantage of the fact that our fingerprints, face, iris, voice, or even our DNA, are publicly available data. This constitutes one of the well-known drawbacks of biometrics, "biometric traits are not secrets" [65], [66], [6], [67].

Such public dimension of biometrics is one of the main reasons for which spoofing has attracted a lot of interest not only from researchers but also from general users, who are very much seduced by the "do-it-yourself" nature of these attacks. It is precisely this characteristic that renders spoofing really dangerous, as it transforms every user into a potential attacker.

The public, low-cost and low-tech features of spoofing are well reported in the literature, where it has been shown in different works that many, if not all biometric modalities, are vulnerable to this threat [68], [59], [69], [70], [71], [72], [73], [74], [75], [76]. Therefore, nowadays the question is not any more whether or not biometrics can be copied or forged, but rather to what extent systems are robust against these attacks and if they incorporate the necessary countermeasures to detect them. However, counterfeiting this type of threats is not a straight forward problem. As they are performed in the analogue domain and the interaction with the acquisition device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective. As a result, specific countermeasures that enable biometric systems to detect fake samples and reject them have to be developed.

The general biometric security context described above, and specifically that related to spoofing, has promoted in the last 10 years a significant amount of research which has flooded journals, conferences and media with new information, methods, algorithms and techniques regarding anti-spoofing approaches that intend to make this technology safer. This has been the case specially for some of the most deployed, popular and mature modalities such as face, fingerprints and iris, which have also been shown to be the most exposed to spoofing. At the moment, the amount of new contributions and initiatives in the area of spoofing requires a significant condensation effort to keep track of all new information in order to form a clear picture of the state of the art as of today.

The present part of the report is intended as a general guide to the spoofing and anti-spoofing field, not focusing on any particular biometric modality. It introduces some important concepts,

terms and classifications that will be later used and applied in Section 3 to the particular case of 3D face recognition spoofing.

## 2.2. Biometric spoofing and anti-spoofing

In spite of some ongoing efforts and proposals to reach a unified and standardized nomenclature for vulnerability related concepts, the biometric community has still not reached a general agreement on the best terminology to be used in each case [80], [81], [42].

In light of the absence of a closed definition, the present technical report will follow the specialised literature where biometric spoofing is widely understood as the ability to fool a biometric system into recognizing an illegitimate user as a genuine one, by means of presenting to the sensor a synthetic forged version (i.e., artefact) of the original biometric trait. Such attacks, also referred to in some cases as direct attacks [33], fall within the larger category "presentation attacks", defined in the latest draft of the ISO/IEC 30107 standard as "presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system" [42]. Such a wider group of attacks also includes the presentation to the acquisition device of human characteristics (and not only synthetic artefacts) such as dead fingers, mutilated traits, real living traits under coercion or a different living trait (i.e., zero-effort impostor attempts that try to take advantage of the False Acceptance Rate, FAR, of biometric systems) [80].

Therefore, spoofing consists in using an artificial trait to impersonate a different user or to create a new genuine identity. Several scenarios are typically conceived for spoofing attacks depending on the type of biometric system considered. i) Verification system: In the most common case, spoofing is carried out at the time of authentication by presenting to the sensor a fake physical copy of the genuine's user trait, which is acquired and matched to the enrolled real template of that genuine user. ii) Verification system/Identification system in closed set: Spoofing may also be performed at the enrolment stage by generating a new identity with an artefact (not necessarily imitating any real user's trait) which can later be used by different people to access the system. iii) Identification system in open set: In this case a new identity is created with the spoofing artefact to avoid being found in a watch list (e.g., to obtain a visa for entering a country where the attacker has the access banned).

Given the above definition for spoofing, an anti-spoofing method is usually accepted to be any technique that is able to automatically distinguish between real biometric traits presented to the sensor and synthetically produced artefacts containing a biometric trait. As in the spoofing case, although it is a very extended one, this nomenclature is not carved in stone and, very often, anti-spoofing approaches are also referred to in the literature as liveness detection or vitality detection techniques. Rigorously speaking, both terms (i.e., anti-spoofing and liveness detection) are not fully equivalent, as not all anti-spoofing methods are necessarily based on cues directly related to living features of the biometric traits. However, in practice, they are used as synonyms in the majority of cases, therefore, in the present document we will not make any difference between them. It is also worth noting that certain anti-spoofing techniques may also be highly effective to detect other types of presentation attacks (e.g., dead or mutilated traits).

Anti-spoofing methods represent a challenging engineering problem as they have to satisfy certain demanding requirements [82]: (i) non-invasive, the technique should in no case be harmful

or require an excessive contact with the user; (ii) user friendly, people should not be reluctant to use it; (iii) fast, results have to be originated in a reduced lapse of time as the user interaction with the sensor should be kept as short as possible; (iv) low cost, a wide use cannot be expected if the cost is excessively high; (v) performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (e.g., false rejection) of the biometric system. From a general perspective, anti-spoofing techniques may be classified into one of three groups depending on the part of the biometric system where they are integrated (see Figure 1):

- **Sensor-level techniques**. Usually referred to in the literature as hardware-based techniques. These methods add some specific device to the sensor in order to detect particular properties of a living trait (e.g., blood pressure, fingerprint sweat, or specific reflection properties of the eye). As shown in Figure 1, such techniques are integrated in the biometric sensor. In general, hardware-based approaches measure one of three characteristics, namely: (i) intrinsic properties of a living body, such characteristics include physical properties (e.g., density or elasticity), electrical properties (e.g., capacitance, resistance or permittivity), spectral properties (e.g., reflectance and absorbance at given wavelengths), or even visual properties (e.g., colour and opacity); (ii) involuntary signals of a living body, such signals can be attributed to the nervous system and good examples are the pulse, blood pressure, perspiration, pupillary unrest (hippus), brain wave signals (EEG) or electrical heart signals; (iii) responses to external stimuli, also known as challenge-response methods, which require the user cooperation as they are based on detecting voluntary (behavioural) or involuntary (reflex reactions) responses to an external signal. Examples of such methods can be the contraction of the pupil after a lighting event (reflex), or the movement of the head following a random path predetermined by the system (behavioural).

  Multibiometric techniques will also be included in this category [83], [34], [84], although, in some cases, they could reasonably be classified as well into the group of feature-level methods (described next). Multibiometric anti-spoofing is based on the hypothesis that the combination of different biometrics will increase the robustness to direct attacks, as, in theory, it is presumed more difficult to generate several fake traits than an individual one. Following this assumption, multimodal approaches fuse more than one modality. Generally, the strategy followed is to combine complementary traits in terms of performance and vulnerabilities, that is, use together a biometric very accurate but also vulnerable to spoofing (e.g., fingerprints) with one harder to fake which presents worse recognition rates (e.g., the finger vein pattern). Such a strategy requires the addition of further hardware acquisition devices at the sensor level, which makes these techniques eligible to be included in the sensor-level group of anti-spoofing methods. Note that the above hypothesis (i.e., circumventing a multibiometric system implies breaking all unimodal modules) has already been shown to be untrue as, in many cases, fooling just one subsystem is enough to gain access to the complete application [85], [86], [75], [87], [88]. Therefore, multibiometry by itself does not necessarily guarantee a higher level of protection against spoofing attacks. As such, specific protection schemes for multibiometric systems have started to be studied recently [32], [89].

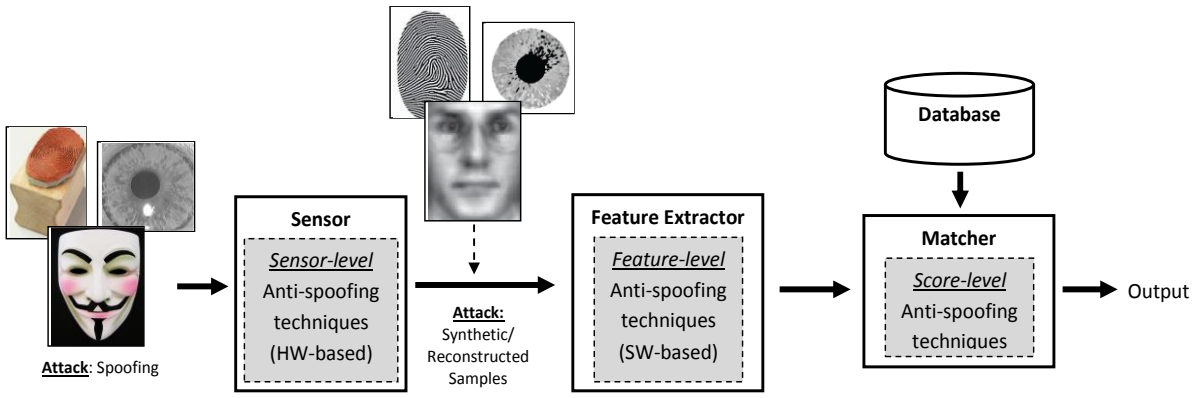


**Figure 1: General diagram of a biometric system specifying the modules where the three types of anti-spoofing techniques may be integrated (sensor-level, feature-level and score-level). Also displayed are the two different type of attacks for which anti-spoofing techniques may offer protection: spoofing and attacks carried out with synthetic or reconstructed samples.**

- **Feature-level techniques**. Usually referred to in the literature as software-based techniques. In this case the fake trait is detected once the sample has been acquired with a standard sensor, that is, features used to distinguish between real and fake traits are extracted from the biometric sample (usually images, as in the case of face, or some kind of time functions, as in the case of speech), and not the human body itself. These methods are installed after the sensor, usually operating as part of the feature extractor module (as shown in Figure 1). They can be further classified into static and dynamic anti-spoofing methods, depending on whether they operate with only one instance of the biometric trait, or with a sequence of samples captured over time [90]. Although they may present some degradation in performance, in general, static features are preferable over dynamic techniques as they usually require less cooperation from the user, which makes them faster and less intrusive. Such a subdivision in static and dynamic approaches is of special interest for instance in face recognition, where there exist systems working on single facial images (e.g., passport picture) and on video sequences (e.g., surveillance camera).

  Although, for clarity, multimodality will be considered in the document as a sensor-level type of anti-spoofing countermeasure, some of these approaches can also be included in the present group. For instance, from just one single high resolution image of a face we may perform both face and iris recognition. In this particular case, a multimodal strategy is being applied at the feature extractor level, with no need of any additional hardware or sensing device. An appealing characteristic of software-based techniques is that, as they operate directly on the acquired sample (and not on the biometric trait itself), they are potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, feature-level methods can protect the system against the injection of reconstructed or synthetic samples2 into the communication channel between the sensor and the feature extractor as depicted in Figure 1 [91], [92], [93].

- **Score-level techniques**. Very recently, a third type of protection methods which fall out of the traditional two-type classification software- and hardware-based, have started to be analyzed in the field of fingerprint anti-spoofing. These protection techniques, much less common than the previous two categories, focus on the study of biometric systems at the

score-level, in order to propose fusion strategies that increase their resistance against spoofing attempts. Due to their limited performance, they are designed as supplementary measures to the sensor-level and feature-level techniques presented above, and are usually integrated in the matcher (as shown in Figure 1). The scores to be combined may come from: i) two or more unimodal biometric modules; ii) unimodal biometric modules and anti-spoofing techniques; or iii) only results from anti-spoofing modules.

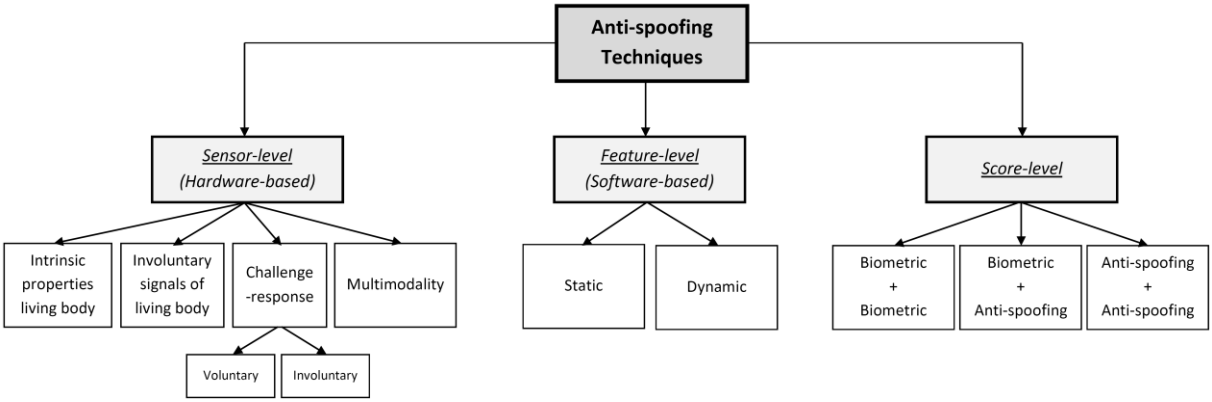


**Figure 2: General taxonomy of anti-spoofing methods considered in the present report with the three main groups depicted in Figure 1: sensor-level, feature-level and score-level techniques.**

A graphical diagram of the categorization proposed above is given in Figure 2. Although the present report will follow this three-group taxonomy, this is not a closed classification and some techniques may fall into one or more of these groups (e.g., as already mentioned, some multibiometric methods could be a good border-line example). Nonetheless, we believe that this taxonomy can help to visualize the current biometric anti-spoofing scene. As well, the reader should be aware that, even though this is a quite extended and accepted classification, others are also possible.

It is also worth highlighting that the three types of anti-spoofing approaches presented here are not exclusive, and may be coupled in order to improve the overall security performance of the system. In fact, the two most deployed types of methods described above (hardware- and software-based), have certain advantages and drawbacks so that, in general, a combination of both would be the most desirable protection strategy to increase the security of biometric systems. As a coarse comparison, sensor-level schemes usually present a higher fake detection rate, while feature-level techniques are in general less expensive (as no extra device is needed), less intrusive and more user-friendly since their implementation is transparent to the user. As already mentioned, score-level protection techniques present a much lower performance and are designed only as a support to the sensor- or feature-level protection measures.

As general reference, Table 1 presents a comparative summary of some of the most relevant characteristics that are desirable in anti-spoofing protection schemes [82], for the three classes considered in the technical report. The table should be understood only as a very broad indication of their capabilities. Therefore, in practice, a specific individual study should be carried out for each proposed anti-spoofing algorithm in order to determine its level of compliance with each of these features.

| HIGH LEVEL COMPARISON OF ANTI-SPOOFING TECHNIQUES | | | | | | |
|---|---|---|---|---|---|---|
| **Type** | **Subtype** | **Performance** | **Low-cost** | **User friendly** | **Non-invasive** | **Protection vs other attacks** |
| Sensor-level | Intrinsic properties | ++ | + | - | - | - |
| | Involuntary signals | ++ | - | - | - | - |
| | Challenge response | ++ | - | - | - | - |
| | Multimod. | + | - | + | + | - |
| Feature-level | Static | + | + | + | ++ | + |
| | Dynamic | + | + | - | - | + |
| Score-level | Biom.+Biom. | -- | + | + | ++ | - |
| | Biom.+Anti-Spoof. | -- | + | + | ++ | - |
| | AS+AS | -- | + | + | ++ | - |

**Table 1: Coarse comparison of the general level of compliance with the requirements defined in [82], of the different types and subtypes of anti-spoofing techniques considered in the report (see Figure 2). In the last column it also appears the potential ability of the anti-spoofing techniques to detect eventual non-spoofing attacks such as the ones carried out with synthetic or reconstructed samples shown in Figure 1.**

## 2.3. Spoofing Evaluation

"In God we trust; all others must bring data". This quote commonly attributed to William Edwards Deming[3] may be applied to the evaluation of any machine learning or pattern recognition problem. Furthermore, these data should be public so that results may be reproduced and fairly compared, in order to avoid reaching the situation so well illustrated by another well-known machine learning principle: give me the performance figure you want to reach and I will provide you the database that meets it.

Certainly, one of the key challenges faced nowadays by the rapidly evolving biometric industry is the need for publicly available standard datasets that permit the objective and reproducible evaluation of different aspects related to biometric recognition systems (e.g., performance, security, interoperability or privacy). This is particularly relevant for the assessment of spoofing attacks and their corresponding anti-spoofing protection methodologies. In relation to spoofing, only recently has the biometric community started to devote some important efforts to the acquisition of large and statistically meaningful anti-spoofing databases. In most cases, these datasets have been generated in the framework of international evaluation competitions such as the series of Fingerprint Liveness Detection Competitions, LivDet, held biennially since 2009 [169], [170], [55], or the more recent 2D Face Anti-Spoofing contests that started in 2011 [151], [54]. Such initiatives

[3] (W.E.D, 1900-1993). On the Web, this quote has been widely attributed to Deming, however, as stated in the introduction of [168]: ironically enough, we could find no "data" confirming this end.

provide public and common benchmarks for developers and researchers to objectively evaluate their proposed anti-spoofing solutions and compare them in a fair manner to other existing or future approaches. This way, the public availability of standardized datasets is fundamental for the evolution of the state of the art.

In spite of the increasing interest in the study of vulnerabilities to direct attacks, the availability of such spoofing databases is still scarce. This may be explained from both a technical and a legal point of view:

- From a technical perspective, the acquisition of spoofing-related data presents an added challenge to the usual difficulties encountered in the acquisition of standard biometric databases (i.e., time-consuming, expensive, human resources needed, cooperation from the donors...): the generation of a large amount of fake artefacts which are in many cases tedious and slow to generate on large scale (e.g., face masks, gummy fingers, or printed iris lenses).
- The regulatory framework related to privacy and data protection are not always well understood by researchers and make the sharing and distribution of biometric databases among different research groups or industries more challenging. As a result, most laboratories working in the field of spoofing have acquired their own proprietary (and usually small) datasets in order to evaluate their protection methods. Although these are very valuable efforts, they have a limited impact, since the results may not be compared or reproduced by other researchers.

Both public and proprietary datasets acquired for anti-spoofing evaluation are generally constructed following one of the next three approaches:

- **Different real/fake users**. The spoofing database is constructed using real samples of a previously existing dataset. Then, fake samples of different new users are added. Anti-spoofing is a two class classification problem, therefore, from a theoretical point of view, such an approach is valid for the evaluation of liveness detection techniques, as the database contains samples of both classes. However, this type of database is not advisable and should be avoided, as it presents two major problems: on one hand, it has the fundamental limitation of not allowing vulnerability studies of spoofing attacks where the intruder tries to access the system using a fake biometric trait of a genuine user (as real and fake samples do not coincide); on the other hand, real and fake samples do not only correspond to different persons but may also have been acquired with a different sensor, at a different location, or following a different protocol, which could potentially lead to biased results. Examples of works using such databases are [28], [171], [172].
- **Same real/fake users, but different acquisition conditions**. As in the previous case, the spoofing database is constructed based on real samples of a previous standard dataset. However, in this case, those real samples are the ones used to produce the fake spoofs, consequently both real and fake users coincide. This could be, for instance, the case of a face spoofing database where the artefacts used to carry out the fraudulent access attempts are printed photographs of an already publicly available real face image database. Again, the problem in this case is that the results of an anti-spoofing evaluation may be biased due to changes in the acquisition environment (e.g., sensor, illumination, distance to the sensor, pose, pressure, size, resolution, etc.) In such conditions, the liveness detection algorithm

may be detecting those contextual variations, and not the intrinsic differences between real and fake samples. Examples of works using such databases include [173], [174], [111].

- **Same real/fake users and same acquisition conditions**. This is the most advisable way to proceed in an anti-spoofing evaluation. In this case, the database is generated from scratch for the same real and fake users, using the same acquisition environment. Most of the works presented in the face literature review and all the competitive anti-spoofing evaluation campaigns follow this approach.

The acquisition of spoofing databases has allowed the organization of several anti-spoofing evaluation competitions. Such competitions, as in other biometric-related scenarios [175], may be classified in two main scenarios:

- **Algorithm-based**, also referred to in the literature as technology evaluation [175], thought to evaluate the liveness detection modules or algorithms on their own, independently of the rest of the system, and therefore well suited to assess feature-level techniques.
- **System-based**, also known as scenario evaluation [175], designed to evaluate the biometric system as a whole, including the scanner, and therefore adequate to assess sensor-level techniques.

The advantage of algorithm-based evaluations is that the same data and protocol may be used to assess all current techniques. Furthermore, this benchmark can be made public, so that future software-based methods may be directly compared to the competition results. This way, the evolution of anti-spoofing performance can be clearly established. On the other hand, system-based evaluations are just restricted to the scope of the competition, and no further comparison may be determined with future systems as new different data would have to be acquired based on each novel sensor. That is, it is not possible to acquire a single distributable database that satisfies the specific necessities of each different current or future sensor-based approaches, due to their intrinsic hardware-based nature.

However, it is important to highlight that, although more difficult than assessing the performance of feature-level techniques, it is still possible to carry out competitive evaluations of complete liveness detection systems (including the acquisition sensor) and not just of a particular anti-spoofing algorithm or module. Such system-based evaluations have already started up at the fingerprint LivDet 2011 and 2013 and at the iris LivDet 2013 competitions [170], [55], [56]. In these three contests, the two evaluation modalities mentioned above were offered to the participants: (i) submission of anti-spoofing software-based algorithms (i.e., only the liveness detection module), that were evaluated on the exact same data and following the exact same protocol (now publicly available); (ii) submission of complete functional biometric systems, that were tested performing a fixed number of real access attempts and spoofing access attempts (i.e., direct attacks), carried out with the same, or very similar artefacts to those used for the generation of the software-based database. In these last case, there are a number of factors that are important to be taken into account in order to obtain comparable results, such as: same spoofs to evaluate all systems, same live subjects, same acquisition conditions (e.g., in the case of face, background, pose or illumination), or control the possible degradation of the spoofs.

Compared to algorithm-based evaluations, system-based ones provide a very good estimation of the real anti-spoofing capabilities of fully functional biometric systems, and not just of the liveness detection algorithm. Such type of assessment also gives very valuable information about the real

resistance against spoofing of commercial biometric applications which, in practice, are released to the market as a complete finalized product and not as independent modules or algorithms. Furthermore, system-based evaluations represent a closer approximation to spoofing attacks that could be carried out in a real-world scenario.

Another important observation worth highlighting in the field of anti-spoofing assessment, is the distribution of fake samples across datasets. Up to now, in all the algorithm-based competitions that have been organised (three in fingerprint, two in face and one in iris), the train and test sets released to the participants contained the same type of spoofs. This means that algorithms may be trained and tuned on the same type of attack data that will later be used for their testing. However, in a real operational scenario, algorithms have to face artefacts which are unknown to them. This way, results obtained under laboratory conditions may be an optimistic estimate of the real performance of the anti-spoofing methods being tested.

This possible bias in the evaluation results between laboratory and real environments was corrected in the systems category of the LivDet 2011 and 2013 competitions. In these two contests, the participants did not receive any training data and were just given some general information about the three types of spoofs that would be used to attack their systems. Then, in the testing phase, in addition to these three known artefacts, two more, totally new for the systems, were also used for evaluation. A similar approach could be followed in algorithms-based assessment by limiting the diversity of fake training data compared to that used for testing.

The spoofing case study conducted by the JRC in the field of 3D face recognition which is thoroughly described in Sect. 3 of the present report, contains both type of evaluations:

- Algorithm-based: two recognition algorithms, one 3D-based and one 2.5D-based, are tested against the same spoofing data previously acquired.
- System-based: a whole commercial system is tested “on the spot” (not using any pre-acquired data) against 3D masks.

For further details on the dataset acquired to perform algorithm-based evaluations and on the system-based test of the commercial system we refer the reader to Sect. 3.3.

# 3. JRC Case study: 3D and 2.5D face recognition spoofing using 3D printed models

## 3.1. Motivation, objectives and contributions

One of the main reasons for which spoofing has attracted all the attention shown in the previous sections, is its "do-it-yourself" dimension. It is well known that absolute security does not exist: given enough funding, willpower and the proper technology, every security system can be compromised. In this context, the objective of security experts is to develop applications such that the funding, the will, and the resources needed by the attacker to bypass them prevent him from attempting to do so. For this reason, protection measures are usually developed first for low-cost, simple, low-tech attacks that are accessible to the general public. Unfortunately, it has already been shown in a significant number of occasions that spoofing falls within this category [5], [11], [7]. Such a "public" or "non-technological" nature of spoofing has thrown, not only researchers, but also users and vendors, to the search of new spoofing-related vulnerabilities and the proposal of innovative anti-spoofing solutions.

In particular, the face modality has been one of the most active biometrics in the field of spoofing. A long way has been covered since the first pioneering works studying the robustness of 2D face recognition to attacks carried out with a simple hard-copy impression of the genuine user's face image [103], to the latest developments involving sophisticated mask attacks [107], [108]. A big contribution to such significant progress has been the acquisition and distribution of public databases where researchers can objectively evaluate following a reproducible protocol novel protection techniques [102], [105]. Several of these databases have been acquired in the context of international competitions which have also boosted the development of technological innovation to counterfeit spoofing [59], [54].

However, in spite of the evident advances that have been reached, more evolved and sophisticated attacking techniques continue to appear for which new protection solutions are needed. In this continuous and relentless race between protection and attack methods, common to all security-related technologies, it is essential to keep track of the rapid technological progress, since some of the advances can be the key to discover new vulnerabilities or to propose novel countermeasures.

For instance, in the field of face spoofing, there is still not enough understanding of the potential risk posed by mask attacks, where the intruder tries to illegally access the system using a 3D model of the genuine user face geometry. In part, the scarcity of research works addressing this potential threat has been due to the technical and economic difficulty posed by the generation of a database of realistic masks. However, these obstacles have been mitigated by some companies where such 3D face models may be ordered[4]. Furthermore, self-manufacturing a face model is also becoming more feasible and easier each day with the new generation of affordable 3D acquisition sensors[5], dedicated scanning software[6] and the price decrease of 3D printing devices[7], which have already

[4] www.thatsmyface.com; https://shapify.me; www.sculpteo.com
[5] http://en.wikipedia.org/wiki/Kinect; http://en.wikipedia.org/wiki/PrimeSense
[6] www.skanect.com; www.kscan3d.com; www.fablitec.com

been used within the field of biometrics to increase the accuracy of fingerprint-based recognition technology through the generation of 3D printed phantom fingerprints [192].

In addition to the above mentioned new spoofing possibilities given by the latest technical advances, other open problems remain largely unexplored in the field of face spoofing. For instance, even though the vulnerabilities of 2D face systems are quite well known, very few research has been yet carried out on the spoofability of 3D and 2.5D face recognition technology, which is resistant to classical attacks carried out with flat surfaces (e.g., printed photographs, images or videos replayed on the screen of a portable device).

The JRC decided therefore to take advantage of the newly available and affordable off-the-shelf 3D sensing, processing and printing technologies, and to provide a comprehensive study on the feasibility of spoofing 3D and 2.5D face recognition systems with low-cost self-manufactured models, reporting a systematic and rigorous evaluation of the real risk posed by such attacking approach.

Therefore, motivated by the current spoofing context presented in Section 2, where extensive research has already been conducted but where many open questions remain, the contributions of the JRC can be summarized as follows:

- Thorough review of the state of the art in face spoofing.
- Presentation of a new face spoofing database which contains 3D, 2.5D and 2D data acquired with two different 3D sensors.
- First vulnerability study of 3D and 2.5D face recognition systems to spoofing attacks carried out with low-cost self-manufactured 3D printed models.

## 3.2. State of the art in face spoofing

Several reasons have driven us to select the face biometric as the focal point of the present spoofing case study:

- According to the International Biometric Group (IBG), face is the second most largely deployed biometric at world level in terms of market quota right after fingerprint [94].
- It is also adopted in most official identification documents such as the ICAO-compliant biometric passport [95] or national ID cards [96]. As such, nowadays face is one of the biometric traits with the highest potential impact both from an economic and a social point of view.
- Together with the fingerprint trait, it is most probably the biometric where the most spoofing-related research has been conducted, leading to a very large amount of published works. However, unlike in the fingerprint case [77], [78], [79], there is still no rigorous and comprehensive survey covering all the anti-spoofing methods proposed in the field of face recognition.

Before reviewing the different works that have been proposed as protection methods against direct attacks (in Section 3.2.2), a summary of the most common spoofing techniques studied to date is presented (in Section 3.2.1). This initial short overview on spoofing can be useful to understand the rationale behind the design of some anti-spoofing techniques later presented and also the structure of the evaluation databases described in the last section of this state of the art

[7] www.sharebot.it/; http://cubify.com

review (Section 3.2.3). This way, the reader can gain a more general perspective on the current panorama in the field of face biometric spoofing. The review of the anti-spoofing techniques follows the general categorization introduced in Section 2.2

### 3.2.1. Face spoofing

The use of masks or facial disguises to avoid being recognized is a practice which has been observed for centuries in the vast majority of known civilizations. Following this trend, probably the most modern version of this long-going tradition to change oneself's physical appearance, is the use of plastic surgery, which is becoming more and more popular thanks to the availability of advanced technology, its affordable cost, and the speed with which these procedures are now performed.

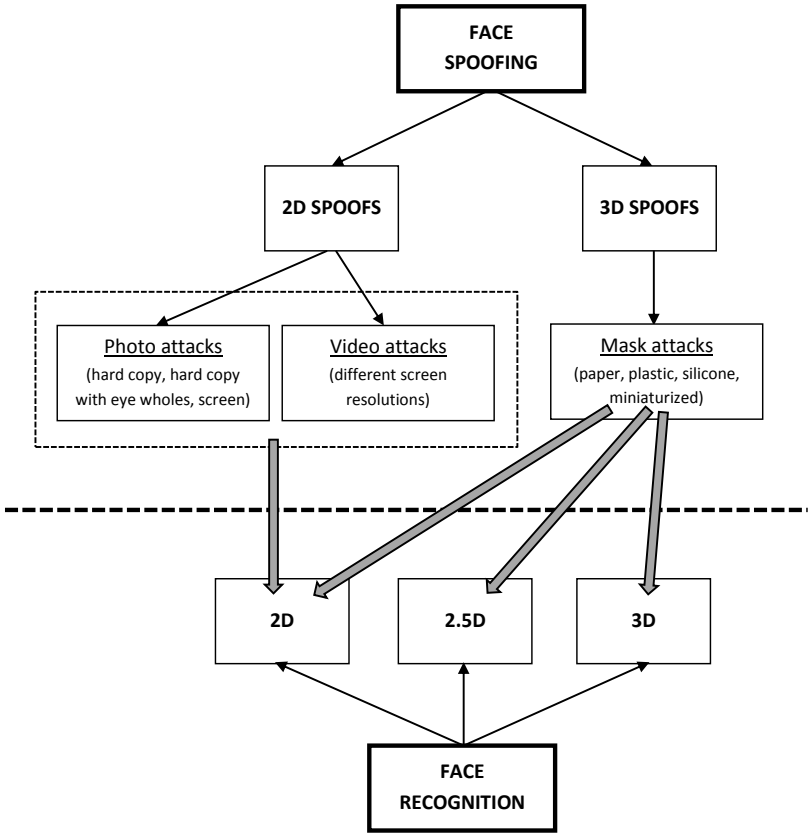


**Figure 3: General classification of face spoofing techniques studied in the literature. For each type of attack the grey arrows indicate to what type of face recognition technology they represent a potential threat.**

Recently, it has been proven that, in spite of some efforts to develop specific algorithms robust to facial surgery changes [97], [98], [99], the problem of recognizing a person after undergoing this type of operations is still an open challenge for automatic face authentication systems [100]. Even without having to turn to irreversible treatments, some works have also shown that face-based biometric systems may be fooled just by wearing regular make-up [101].

Such techniques are usually used to hide the user's own identity (i.e., Bob denies being Bob) and not to perform an attack in which Bob tries to impersonate John. However, it has recently been shown at a live demonstration in a biometric-dedicated conference that this security scenario could change, and that methods such as surgery or make-up may be successfully used to perform direct

attacks. In this conference, a female intruder was able to access a face recognition system in the place of a male user just by wearing some adequate make-up [16].

Apart from these still limited examples on the potential use of disguise techniques for spoofing purposes, the vast majority of face direct attacks reported in the literature may be classified in one of two groups, as shown in Figure 3, depending on whether the artefacts used are: *i*) 2D surfaces (e.g., photo, video) which are successful against 2D face systems (see grey arrows in Figure 3), or *ii*) 3D volumes (e.g., masks) which may be used to attack 2D, 2.5D and 3D face recognition technology. Such artefacts have been used to carry out three main types of attacks which present an increasing level of spoofing potential:

- **Photo Attacks**. These fraudulent access attempts are carried out presenting to the recognition system a photograph of the genuine user. The photograph may have been taken by the attacker using a digital camera, or even retrieved from the internet after the user himself uploaded it to one of the very popular online social networks available today [67].
  The image can then be printed on a paper (i.e., print attacks, which were the first to be systematically studied in the literature) or may be displayed on the screen of a digital device such as a mobile phone or a tablet (i.e., digital-photo attacks) [15], [102], [59]. A slightly more advanced type of photo-attack that has also been studied is the use of photographic masks, which are high resolution printed photographs where the eyes and the mouth have been cut out, and the impostor is placed behind [103], so that certain face movements such as the eye blink may be reproduced.
- **Video Attacks**. Also referred to in some cases as *replay attacks*. They represent a more sophisticated version of the simple photo spoofs. In this case, the attacker does not use a still image, but replays a video of the genuine client using a digital device (e.g., mobile phone, tablet or laptop) [104], [105]. Such attacks appeared as a further step in the evolution of face spoofing and are more difficult to detect, as not only the face 2D texture and structure, but also its motion and dynamics are copied.
- **Mask Attacks**. In these cases the spoofing artefact is a 3D mask of the genuine client's face, increasing the difficulty to find accurate countermeasures against them. As the whole 3D structure of the face is imitated, the use of depth cues which could be a solution to prevent the previous two types of attacks (carried out with flat surfaces), becomes inefficient against this particular threat.
  Although the possibility to bypass a biometric system wearing a mask imitating the face of a different user is an idea that has been circulating for some time [106], this type of attacks is far less common than the previous two categories and is only starting to be systematically studied with the acquisition of the first mask-specific datasets [107], [108], where different materials and sizes have been considered to produce the masks [109], [110].

In addition, all the previous types of attacks have a number of variants depending on the resolution of the attack device, the type of support used to present the fake copy (e.g., handheld or fixed support), or the type of external variability allowed (e.g., illumination or background conditions). These different attack versions may be found in the various face spoofing databases available for research [102], [111], [59], [54], [105], [107], [108], which will be reviewed in Section 3.2.3.

It is also worth highlighting that face recognition systems may also be subjected to attacks from identical twins claiming to be the same person. Strictly speaking these are not spoofing attacks (as there is no physical artifact involved) but rather zero-effort impostor attempts in which a given user A presents his own biometric while trying to access the system as user B. Although some of the anti-spoofing techniques that will be reviewed in the following sections could potentially be used against this particular vulnerability, it will not be treated in the present technical report. We refer the interested reader to some specific works on this topic to understand the implications and performance of face recognition systems in the presence of twins [112], [113], [114], [115].

### 3.2.2. Face anti-spoofing

***1) Face Anti-spoofing: Feature level dynamic approaches:*** Although the first face anti-spoofing works date back more than a decade [129], it has not been until the last three years that this technology has experimented a real revolution under the umbrella of the TABULA RASA European project focused on spoofing attacks to biometric systems [64]. Another decisive factor for the development of new protection methods against direct attacks has been the distribution of several public face spoofing databases which have made possible for researchers to focus on the development of efficient countermeasures and not on data acquisition issues [102], [105], [104], [107]. Both factors have favoured the recent publication of multiple techniques in 2D face anti-spoofing and even to initiate a promising research line in new protection algorithms for 3D face recognition systems against mask attacks.

One of the pioneer feature-level protection approaches in 2D face recognition appeared as a countermeasure to the first attacks studied which made use of static face printouts (i.e., print attacks). Such anti-spoofing techniques, which still remain quite popular against these fraudulent access attempts, rely on the detection over a video sequence of face motion. In particular, they are based on the trajectory analysis of specific parts of a live face. These dynamic features reveal valuable information to discriminate between real faces and spoofed static copies. Typical cues used in this type of anti-spoofing methods, some of them involving challenge-response strategies, are eye blink [130], [123], [131], [132] or other face and head gestures detected trough face and gaze tracking [133], [134] or estimating the optical flow [103], [135], [27], [136]. These techniques are usually highly effective to detect photo-attacks but lose accuracy against illegal access attempts carried out with replayed videos where not only the face appearance but also its movements are forged.

In order to overcome this shortcoming, some dynamic liveness detection techniques have been specifically proposed to detect video-based attacks: exploiting the 3D structure of the face through the analysis of several 2D images with different head poses [124], [137]; using context-based analysis in order to take advantage of non-facial information available from acquired samples such as motion features from the scene (e.g., background *vs* foreground motion) [138], [139], [59], [140]; estimating the noise produced by the recapturing process (i.e., fixed pattern noise and the noise resulting from the photo-responsiveness of non-uniform light-sensitive cells) [141]; using modified versions of the Local Binary Patterns (LBP), in order to also take into account temporal information present in video sequences [125] or to analyse the dynamics of facial texture in comparison to rigid objects such as photos or masks [142]; applying the recently proposed Eulerian video magnification algorithm to enhance the motion in a video as a previous step to anti-spoofing feature extraction [126].

Given that they are designed to exploit both spatial and temporal information of face videos, such dynamic-based antispoofing schemes usually present quite high performance rates. However, as a limitation, they cannot be used in systems where only a single face image of the user is available (e.g., passport related applications). Moreover, even in the cases where video data has been recorded (e.g., surveillance applications), it is not rare to find that only a very few non-consecutive frames are suitable for facial analysis, which also limits the final use and accuracy of dynamic-based anti-spoofing approaches.

***2) Face Anti-spoofing: Feature level static approaches:*** The previous non negligible restriction of dynamic anti-spoofing schemes (i.e., need for a temporal sequence of a certain duration), has motivated the appearance of a second group of approaches for the detection of spoofing access attempts to 2D face recognition systems focused on the analysis of a single static image and not of video data. These techniques are in general faster than their dynamic counterparts and, therefore, more convenient for the user, at the cost, in some cases, of a certain performance loss. The vast majority of these methods are based on the analysis of the face texture using different image processing tools such as: the Fourier Spectrum [143]; multiple Difference of Gaussian (DoG) filters to extract specific frequency information [105] which has also been combined with features obtained from the Lambertian model [102] proving a remarkable performance even under bad illumination conditions [111]; partial least squares to analyse specific information from low-level descriptors [144]; combination of low-level and high-level face component descriptors [145]; a more recent trend based on the use of Local Binary Patterns (LBP) to detect photo-attacks [146], [104], which has been successfully combined with other texture descriptors such as Gabor Wavelets and with shape related information extracted using Histogram Oriented Gradients (HOG) in [127]; searching for paper microtextures of print-attacks either by analysing the specular components of the facial image [147] or by using LBPs as features [148], [104]; as in the case of video sequences, context-based approaches have also been proposed for the static scenario focusing in this case not on motion cues, but on the detection of the upper body of the user and the attack support (e.g., paper or tablet) [128]; or evaluating the pixel difference between two consecutive pictures taken with different focus values [149] (although this last method requires two different face images, we include it in the static category as it does not use any temporal information).

These static-based anti-spoofing approaches may as well be applied to the case in which a video sequence is available. In this scenario, the analysis is performed on a frame-by-frame basis, using fusion techniques in a later stage, to combine the individual scores obtained from each frame in order to generate a unique final score or decision (e.g., majority voting). Although such a strategy is feasible, in general, it is less efficient than the schemes specifically designed to work with videos, as no temporal information is exploited (e.g., such as the trajectories of facial features).

Some of the previous techniques have been successfully fused at feature level showing an increase in the accuracy compared to individual parameters [119], [150]. Moreover, a comparative study of several of these dynamic and static approaches may be found in the 2011 and 2013 Competitions on Countermeasures to 2D facial spoofing attacks [151], [54], where it was shown that, wherever possible (i.e., scenarios with availability of facial video data), the feature-level fusion of both types of techniques (static and dynamic) draws the best performance. Further reading on the results and databases used in these competitions may be found in Section 3.2.3.

| FACE ANTI-SPOOFING TECHNIQUES: GENERAL OVERVIEW | | | | | |
|---|---|---|---|---|---|
| **Sensor-level techniques** | | | | | |
| **Reference** | **Subtype** | **Features and methodology** | **Attack** | **Database** | **Error** |
| 2005, Chetty and Wagner [116] | Multibio. | Face + Voice | Video | Public, VidTIMIT DB [117] (43 identities, 500 samples) and UCBN DB [118] (30 identities, 30 samples) | 2% |
| 2008, Kollreider et al. [119] | Challenge-response | Motion detection | Photo, video | Proprietary, 15 identities, 390 samples | 3.5% |
| 2011, Zhang et al. [120] | Intrinsic Property | Reflectance using multispectral lighting in 2D images | Photo, video, mask | Proprietary, 40 identities, 1,000 samples | 7% |
| 2013, Kose and Dugelay [121] | Intrinsic Property | Reflectance in 3D scans | Mask | Proprietary, 20 identities, 400 samples | 5.5% |
| 2013, Dhamecha et al. [122] | Invol. signal | Thermal images | Mask | Public (still to be released), 75 identities, 1,362 samples | 13% |
| **Feature-level techniques** | | | | | |
| **Reference** | **Subtype** | **Features and methodology** | **Attack** | **Database** | **Error** |
| 2007, Pan et al. [123] | Dynamic | Eye blink detection using Conditional Random Fields (CRF) | Photo | Public, NUAA Photograph Imposter DB [102], 15 identities, 75 samples | 2% |
| 2009, Kollreider et al. [27] | Dynamic | Face motion detection using Optical Flow of Lines (OFL) | Photo | Proprietary, 100 identities, 800 samples | 0.5% |
| 2011, Anjos et al. [59] | Dynamic | Context-based using correlation between face motion vs background motion | Photo | Public, PRINT-ATTACK DB [59], 50 identities, 400 samples | 10% |
| 2012, Marsico et al. [124] | Dynamic | 3D structure inferred from 2D images using geometric invariants | Photo | Public, NUAA Photograph Imposter DB | 0.3% |
| 2012, Freitas et al. [125] | Dynamic | Dynamics of the facial texture using LBPs | Photo, video | Public, REPLAY-ATTACK DB [104], 50 users, 1,000 samples | 7.5% |
| 2013, Bharadwaj et al. [126] | Dynamic | Motion detection using Histogram of Oriented Optical Flows (HOOF) after video Eulerian magnification | Photo, video | Public, REPLAY-ATTACK DB | 1.2% |
| 2010, Tan et al. [102] | Static | Face texture using the Lambertian model | Photo | Public, NUAA Photograph Imposter DB | 15% |
| 2012, Zhiwei et al. [105] | Static | Face texture frequency analysis using Difference of Gaussians (DoG) filters | Photo, video | Public, CASIA Face Anti-Spoofing DB [105], 50 identities, 600 samples | 15% |
| 2012, Chingovska et al. [104] | Static | Face texture using LBPs | Photo, video | Public, REPLAY-ATTACK DB, NUAA Photograph Imposter DB, CASIA Face Anti-Spoofing DB | 15% |
| 2012, Maatta et al. [127] | Static | Texture + Shape combining LBPs + Gabor Wavelets + HOG | Photo | Public, NUAA Photograph Imposter DB, REPLA- ATTACK DB, YALE-RECAPTURED DB [111] (10 users, 2,500 samples) | 0.5% |
| 2013, Komulainen et al. [128] | Static | Context-based using upper body and spoof support detection | Photo, video | Public, NUAA Photograph Imposter DB, CASIA Face Anti-Spoofing DB | 3% |

**Table 2: Summary of the most relevant face anti-spoofing techniques presented in Section 3.2.2. The column ``subtype'' corresponds to the algorithm subtype within each of the three main categories considered in the work (sensor-level, feature-level and score-level) as shown in the taxonomy in Figure 2. The column ``attack'' refers to the type of face spoofing attacks considered in the work as defined in Section 3.2.1: photo, video or mask attacks. For clarity, public databases are just referenced the first time they appear in the table, in successive entries only their name is given (for further information on these public databases please see Section 3.2.3). Sizes of databases that appear in column ``database'' are approximate and are given just as an indication of their order of magnitude (for the exact structure and size the reader should consult the corresponding reference). The same applies for results, as the ones shown in the table are an approximation of the different scenarios considered in each work.**

***3) Face Anti-spoofing: Sensor level approaches:*** Regarding sensor-level anti-spoofing techniques, the number of contributions is still not comparable to that of software-based approaches, however, some interesting methods have been proposed base on imaging technology outside the visual spectrum, such as: complementary infrared (IR) or near infrared (NIR) images, which are even claimed to provide sufficient information to distinguish between identical twins [152], [129]; comparing the reflectance information of real faces and fake materials using a specific set-up of LEDs and photodiodes at two different wavelengths [106], [120].

In addition to the previous works, there are other technologies, first proposed for face recognition purposes, that could also be used as sensor-level anti-spoofing techniques. Although no rigorous study has yet been carried out regarding their performance under liveness detection scenarios, such potentially useful mechanisms for 2D face anti-spoofing would include the use of thermal imaging [153], [154], the detection of the facial vein pattern [155], or 3D face acquisition systems [156]. For instance, 3D sensors should be very robust against attacks carried out with flat surfaces (e.g., photo or video attacks) as no depth information would be available. On the other hand, their performance detecting mask-attacks has just started to be investigated using texture analysis inspired on similar 2D protection methods based on LBPs [157], [158] and also on the analysis of the reflectance components that may be computed both from 2D textures and from 3D scans [121]. Similarly, systems based on the detection of the face thermogram would be, in principle, very accurate detecting all three types of major face spoofing attacks (i.e., photo, video and mask attacks) as it is expected that no thermal difference would be visible across fake faces. Some initial efforts to study thermal imaging for liveness detection have already been carried out [159], including the acquisition of a significantly large database of thermal images for standard and disguised access attempts where very promising results have been obtained [122]. Still, it would be necessary to capture further data of face thermograms under normal operational conditions and under spoofing attacks in order to validate these initial findings.

In any case, the fact that these techniques (i.e., 3D and thermal face recognition) already present solid backgrounds for personal authentication, can be an added advantage for their development as security enhancing alternatives, as both tasks (i.e., recognition and anti-spoofing) could be performed from the same sample.

As part of sensor-level liveness detection approaches, multimodality has also been explored. Many of multibiometric antispoofing techniques consider the combination of face and voice, as the latter represents an easily measurable trait. Such methods exploit the correlation between the lips movement and the speech being produced [160], [161], [116], [162], or add specific information obtained from the lip movement in the utterance of a preassigned pin code [163]. The latter method could also be categorized as a challenge-response technique as the user is asked to respond to a system command. Such a challenge-response strategy considering voluntary eye blinking and mouth movement following a request from the system was also studied in [119].

***4) Face Anti-spoofing: Score level approaches:*** Recently, some research has also started in the field of score-level antispoofing strategies for 2D face recognition systems. In one of these first works, the authors study the impact of anti-spoofing measures on the performance of practical face recognition systems. To this end, they analyse different score fusion techniques for the protection and authentication modules under a three-case classification scenario: clients, impostors and attacks [164]. In addition, several fusion strategies for the combination of outputs from anti-spoofing modules have been analysed in order to reduce the performance gap that can be observed, even for

the same protection algorithm, when the evaluation database is changed [165]. In the same line, the combination of scores given by video-based and texture-based anti-spoofing approaches has also been considered in [166], [167], showing great degree of complementarity and a very significant improvement with respect to the individual systems, even for very simple classifiers.

In order to give an overall perspective of the different methods studied so far in the face anti-spoofing related literature, Table 2 presents a general overview of some illustrative works referenced in the present section. The table should be understood as a tool for quick reference and in no case as a strict comparative study, as many of the results shown in the last column have been obtained using proprietary databases designed to evaluate a specific method (see column "Database"). Moreover, in general, these databases are too small to obtain statistically meaningful results and are in most cases presented in their respective works only as a proof of concept. The table objective is to schematically show the most relevant characteristics (i.e., type of anti-spoofing system, type of features used, evaluation database, results, etc.) of several representative articles, in order to help the reader to gain, at a glance, an overall perspective of the different approaches studied so far in the field of face anti-spoofing. For an exhaustive and complete list of all published articles in the area the reader should refer to the inline text in this Section 3.2.

As it may be observed from the information displayed in Table 2, the use of public datasets in facial-related studies is quite generalized. This has allowed comparing results from different works in a fair manner, providing this way a clearer picture of the state of the art evolution, compared to other traits such as fingerprints where many works use proprietary ad-hoc acquired data. For further reading on face anti-spoofing evaluation, publicly available datasets and comparative results from the face anti-spoofing competitions organized so far, the reader is referred to the following Section 3.2.3.

### 3.2.3. Face spoofing evaluation databases

Currently there are six large public face anti-spoofing databases that comprise most of the known types of attacking scenarios described in Section 3.2.1: the NUAA PI DB, the YALE-RECAPTURED DB, the PRINT-ATTACK DB, the CASIA FAS DB, the REPLAY-ATTACK DB and the 3D MASK-ATTACK DB (described in the following subsections). The chronology of all six databases illustrates in a very good manner the state of the art evolution in the field of face spoofing and anti-spoofing, showing how the attacks have become gradually more sophisticated and how the protection methods have adapted to the new challenges in order to increase their efficiency.

The first effort to generate a large and public face anti-spoofing DB was reported in [102] with the NUAA PI DB, which contains only still-images of real access attempts and print-attacks of 15 users. The YALE-RECAPTURED DB appeared soon after, and added the difficulty of having varying illumination conditions as well as considering LCD spoofs (i.e., the attacks were carried out showing the face images on LCD screens) instead of the classic print attempts [111]. This database, however, is still quite restricted in terms of number of users (10), and it only comprises static real and fake images. Furthermore, it presents the drawback of having been captured from an already existing dataset (the Yale Face DB-B), with the limitations that this entails as discussed in Section 2.3. The PRINT-ATTACK DB represents yet another step in the evolution of face spoofing, both in terms of size (50 different users were captured) and of data acquired (it contains video sequences instead of still images). However, it still only considers the case of photo attacks [59]. This feature is improved by

both the REPLAY-ATTACK DB [54] and the CASIA FAS DB [105], which contain not only photo attacks with different supports (e.g., paper, mobile phones and tablets) but also replay video attacks. In addition, this last two databases are complementary, as the REPLAY-ATTACK DB was acquired with one single sensor using different attack devices of increasing quality under varying illumination and background conditions, while the CASIA FAS DB was captured with different sensors under a uniform acquisition setting. To date, the last contribution in the field of public face spoofing databases, is the 3D MASK-ATTACK DB [107], which has initiated the path of 3D face acquisition under mask attacks (all previous datasets comprise only 2D data and photo or video attacks). Table 3 shows a comparison of the most important features of these six face spoofing databases.

| | **COMPARATIVE SUMMARY: PUBLIC FACE SPOOFING DBs** | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Overall Info. (Real/Fake)** | | | **Sensor Info.** | | | | | **Types** | | | **Supp.** | | **Illum.** | |
| | #IDs | #Samp | Type | # | LQ | SQ | HQ | 3D | Ph | Vd | Mk | Hh | Fx | Cont. | Adv. |
| NUAA PI DB [102] | 15/15 | 5,105/ 7,509 | Images | 1 | | X | | | X | | | X | | | X |
| YALE-RECAPT DB [111] | 10/10 | 640/ 1,920 | Images | 2 | | X | X | | X | | | | X | X | X |
| PRINT-ATTACK DB [59] | 50/50 | 200/ 200 | Videos | 1 | X | | | | X | | | X | X | X | X |
| CASIA FAS DB [105] | 50/50 | 150/ 450 | Videos | 3 | X | X | X | | X | X | | X | | | X |
| REPLAY-ATTACK DB [104] | 50/50 | 200/ 1,000 | Videos | 1 | X | | | | X | X | | X | X | X | X |
| MASK-ATTACK DB [107] | 17/17 | 170/ 85 | Videos | 2 | | X | | X | | | X | X | | X | |

**Table 3: Comparative summary of the most relevant features corresponding to the six face spoofing databases described in Section 3.2.3. # indicates number, Samp stands for samples, LQ for 2D Low Quality, SQ for 2D Standard Quality, HQ for 2D High Quality, Ph for photo, Vd for video, Mk for mask, Hh for handheld, Fx for fixed, Cont for controlled and Adv for adverse.**

From the six previous databases, the REPLAY-ATTACK DB is probably the most significant one, not only for its size, multiple and well defined protocols, and types of attacks covered, but also because it was used in the last edition of the Competition on Countermeasures to 2D Facial Spoofing Attacks held in 2013 [54]. For these reasons, as an illustrative example of spoofing attacks carried out against face recognition systems, in Figure 4 we show some typical images (frames extracted from the videos) of real and fake access attempts from the REPLAY-ATTACK DB.

For completeness, the results of the 2013 competition on Countermeasures to 2D Facial Spoofing Attacks are shown in Table 4, in terms of the percentage of correctly classified samples. All the information has been directly extracted from [54]. We refer the reader to that work for further details on the competition.

The contest only considered an algorithm-based evaluation, therefore, only feature-level approaches were submitted (see Section 2.3 for a classification and characteristics of the different possible anti-spoofing evaluations). The competition database (a subset of the REPLAY-ATTACK DB) was divided into: a train set, to tune and train the algorithms; a development set, to fix the decision threshold between real and fake; and a test set, where the final results were computed. The same type of spoofs was present in all three sets.

| | RESULTS 2D FACE ANTI-SPOOFING 2013<br>CORRECTLY CLASSIFICATION RATE (%) | | |
|---|---|---|---|
| | **Static** | **Dynamic** | **100-HTER (test)** |
| Alg1 | X | X | 100.0 |
| Alg2 | | X | 90.9 |
| Alg3 | X | X | 97.5 |
| Alg4 | X | X | 100.0 |
| Alg5 | X | | 98.7 |
| Alg6 | X | | 98.7 |
| Alg7 | X | | 88.0 |
| Alg8 | X | | 84.4 |

**Table 4: Results obtained by the 8 algorithms that participated in the 2013 competition on countermeasures to 2d facial spoofing attacks. HTER stands for half total error rate. For a more detailed description of the database used in the evaluation please see Section 3.2.3. The information displayed in the table has been directly extracted from [54].**

The last column of Table 4 shows, in percentage, the accuracy of the algorithms on the test set computed as 100-HTER, where the HTER is the Half Total Error Rate. The previous two columns indicate if the corresponding anti-spoofing method uses static or dynamic features. From the results, it may be observed that the fusion of the two types of features draws the best results, with the two top algorithms reaching a 100% accuracy even under the multiple attack scenario that was featured in the competition: several illumination and background conditions, different types of spoof devices (print, mobile phone, tablet) and different attacking methods (photo, video). Interestingly, the best static-based algorithms are able to perform almost at the same level as the fused approaches, with a 99% classification rate, significantly higher than the only dynamic technique that was presented to the competition, algorithm 2, which obtained a 91% accuracy.

**1) NUAA PI DB**: The NUAA Photograph Imposter DB [102] is publicly available from the Pattern Recognition and Neural Computing Group of the Nanjing University of Aeronautics and Astronautics (ParNeC-NUAA)[8]. This database contains still images of both real-access and spoofing attack attempts of 15 subjects. The samples are extracted from videos captured with a cheap generic webcam (the model is not specified) which produces standard quality images of 640×480 pixels. The database was acquired in three different sessions separated two weeks from each other under uncontrolled illumination conditions. The amount of data among sessions is unbalanced as not all the subjects participated in the three acquisition campaigns.

For the real access attempts, the subjects were asked to stay as still as possible with no evident face movements such as eye blinking in order to simulate to the larger extent the characteristics of a typical print attack. All the attacks were carried out with printed copies of high definition face close-ups of the users, captured with a standard Canon camera (model is not specified). Three different hard-copies of each photograph were generated to try to spoof the system: i) professional developing on photographic paper of size 6.8cm×10.2cm; ii) professional developing on

[8] http://parnec.nuaa.edu.cn/xtan/data/NUAAImposterDB.html

photographic paper of size 8.9cm×12.7cm; ii) home generated printed A4 70gr copy using a standard color ink HP printer. During the attacks the printed images were moved in different forms, trying to imitate the typical behaviour of real access attempts: back and forth, vertically and horizontally, warped around in the vertical and horizontal axis. The database is divided into a train and test set: the train set comprises images from the two first acquisition sessions, while the test set only contains samples of the last one, therefore there is no overlap between them in terms of samples. However, some users do appear in both sets.

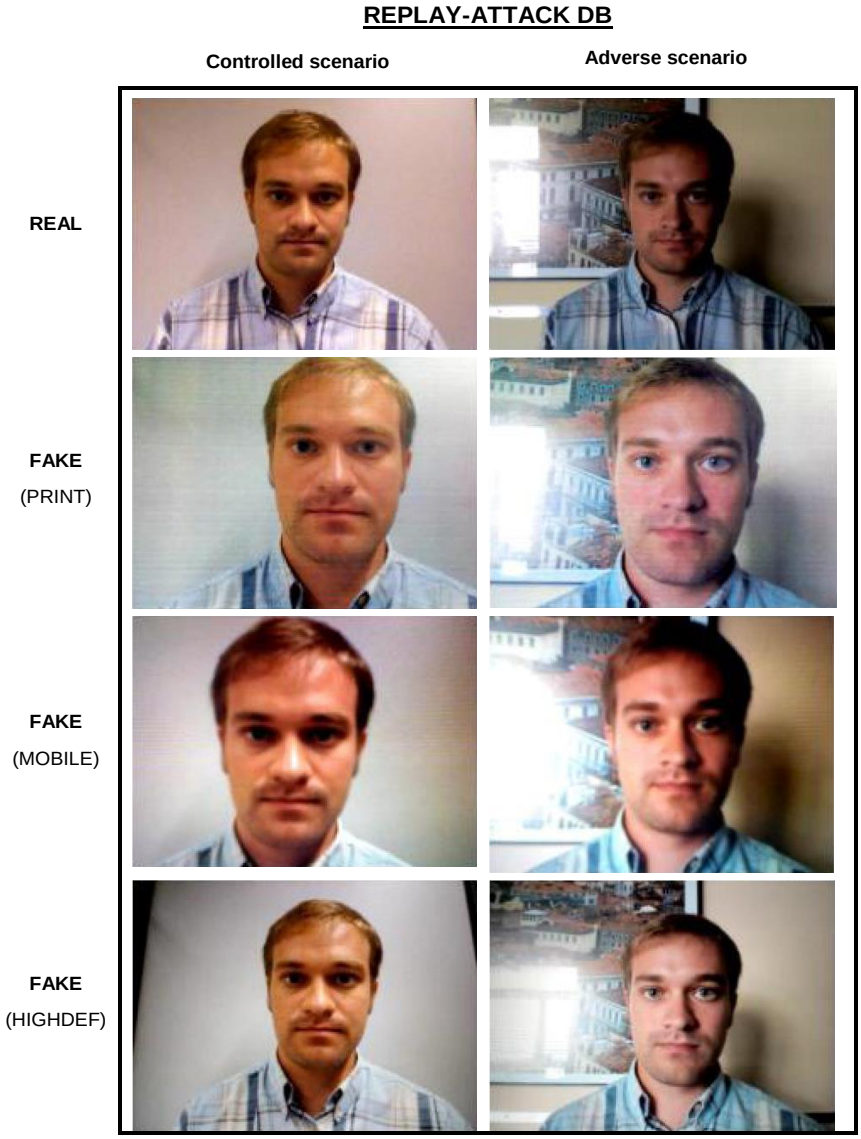


**Figure 4: Typical examples of real and fake (mobile, print and highdef attacks) face images that can be found in the public REPLAY-ATTACK DB. Images were extracted from videos acquired in the two illumination and background scenarios: controlled and adverse. For further details on the types of attacks and acquisition settings please see Section 3.2.3.**

**2) YALE-RECAPTURED DB**: The YALE-RECAPTURED database [111] is publicly available under request from the University of Campinas[9].

The dataset consists of 640 static images of real access attempts and 1,920 attack samples, acquired from 10 different users. The genuine subset is taken from the previously existing Yale Face DB-B [176], where each user was acquired under 64 different illumination conditions.

The attack attempts were carried out displaying the real images on three different LCD monitors: i) LG Flatron L196WTQ Wide 19", ii) a CTL 171Lx 1700 TFT, and iii) a DELL Inspiron 1545 notebook. Then the images were recaptured with two different cameras, a Kodak C813 with a resolution of 8.2 megapixels and a Samsung Omnia i900 of 5 megapixels. After the recapture, the samples were cropped and normalized to grey-scale images of size 64×64.

The multiple illumination conditions make this database a quite challenging one. However, since the genuine and fake subsets were acquired in different settings and with different devices, the results obtained on it may be biased due to these contextual differences.

***3) PRINT-ATTACK DB**:* The PRINT-ATTACK database [59] is publicly available from the IDIAP Research Institute website[10]. This database was used on the 2011 Competition on Countermeasures to 2D Facial Spoofing Attacks [151]. It consists of 200 videos of real accesses and 200 videos of print attack attempts from 50 different users. The database is divided into train, development and test sets which coincide with those used in the 2011 competition.

Real and attack access video sequences were captured with a 320×240 pixel (QVGA) resolution camera of a MacBook laptop, at 25 frames-per-second with an average duration of around 10 seconds and stored in *.mov* format. Videos were recorded under two different background and illumination conditions: *i*) *controlled*, with a uniform background and indoor homogeneous lighting coming from a fluorescent lamp; *ii*) *adverse*, in this case the background is not uniform (regular office-like background) and the scene has day-light illumination.

The attacks were carried out with hard copies of high resolution photographs of the 50 users printed on plain A4 paper with the Triumph-Adler DCC 2520 color laser printer. The photographs were taken during the real access attempts, under the exact same illumination and background setting, with a 12.1 megapixel Canon PowerShot SX150 IS camera. For the attacks the printouts are held in front of the acquisition sensor (i.e., MacBook laptop camera) using two different strategies or supports: hand-held attack (i.e., the intruder holds the photograph with his hands) or fixed support attack (i.e., the picture is stuck to the wall so that there is no movement).

***4) CASIA FAS DB**:* The CASIA Face Anti-Spoofing DB [105] is publicly available from the Chinese Academy of Sciences (CASIA) Center for Biometrics and Security Research (CASIA-CBSR)[11].

This database contains short videos (around 10 seconds in avi format) of both real-access and spoofing attack attempts of 50 subjects, divided into a train and test set with no overlap between them (in terms of users and samples). The samples were acquired with three devices with different resolutions: *i*) *low resolution*, with an old 640×480 USB web camera (model is not specified); *ii*) *normal resolution*, with a modern 480×640 USB web camera (model is not specified); and *iii*) *high resolution*, using the 1920×1080 Sony NEX-5 high definition camera.

[9] http://www.ic.unicamp.br/rocha/
[10] http://www.idiap.ch/dataset/printattack
[11] http://www.cbsr.ia.ac.cn/english/index.asp

Three different types of attacks were considered: *i*) *warped*, illegal access attempts are carried out with slightly curved hard copies on copper paper (which has a higher quality than regular A4 printing paper) of high-resolution digital photographs of the genuine users (taken with the Sony NEX-5 camera); *ii*) *cut*, the attacks are performed using hard copies of high-resolution digital photographs of the genuine users (as before), where the eyes have been cut out and the face of the attacker is placed behind (i.e., so that eye blinking is forged); *iii*) *video*, in this case the high resolution videos of the genuine users are replayed in front of the acquisition device using an iPad.

***5) REPLAY-ATTACK DB****:* The REPLAY-ATTACK DB [104] is publicly available from the IDIAP Research Institute website[12].

The database was acquired as an extension of the PRINT-ATTACK DB, therefore it also contains short videos (around 10 seconds in *.mov* format) of both real-access and spoofing attack attempts of 50 different subjects, acquired with a 320 _ 240 resolution webcam of a 13-inch MacBook Laptop. The recordings were carried out under two different conditions: *i*) *controlled*, with a uniform background and artificial lighting; and *ii*) *adverse*, with natural illumination and non-uniform background.

In this case three different types of attacks were considered with an increasing level of resolution: *i*) *print*, illegal access attempts are carried out with hard copies of high-resolution digital photographs of the genuine users (this data subset corresponds to the PRINT-ATTACK DB); *ii*) *mobile*, the attacks are performed using photos and videos taken with the iPhone using the iPhone screen; *iii*) *highdef*, similar to the mobile subset but in this case the photos and videos are displayed using an iPad screen with resolution 1024×768.

In addition, access attempts in the three attack subsets (mobile, print and highdef) were recorded in two different modes depending on the strategy followed to hold the attack replay device (mobile phone, paper or tablet): *i*) *hand*-based, and *ii*) *fixed*-support.

The database is distributed with an associated protocol which divides the database into train, development and test sets with no overlap between them (in terms of users and samples). The database also contains an enrollment subset with 100 videos corresponding only to real access attempts thought solely for the performance evaluation of the face recognition systems whose vulnerabilities to spoofing attacks will be later evaluated on the rest of the database.

The 2013 edition of the Competition on Countermeasures to 2D Facial Spoofing Attacks was held using a subset of all the available attacks on the REPLAY-ATTACK DB (not just the print data as in the 2011 edition). The exact data and protocol followed on this second edition are also released with the database [54]. The results of the competition are given in Table 4.

***6) 3D MASK-ATTACK DB****:* The 3D MASK-ATTACK DB [107] is publicly available from the IDIAP Research Institute website[13]. It constitutes the first public database that considers mask attacks and that, in addition to the usual 2D data, provides as well depth information. It comprises genuine and attack access attempts of 17 different users. The attacks were performed by one single operator wearing the life-size 3D masks of the genuine subjects, manufactured using the service provided by ThatsMyFace.com[14], which only requires a frontal and two profile pictures of each person to

[12] https://www.idiap.ch/dataset/replayattack
[13] https://www.idiap.ch/dataset/replayattack
[14] http://www.thatsmyface.com/

generate a 3D mask. These three pictures (frontal and profiles) are also distributed with the database.

The database was captured in three different sessions: two real-access sessions held two weeks apart and a third session in which the mask attacks were performed. In each session and for each user, five videos of 10 seconds were captured using the Microsoft Kinect for Xbox 360. This sensor provides both regular 2D RGB data (8-bit) and depth data (11-bit), with resolution 640×480 pixels at 30 frames per second.

Therefore, the data available are: 255 color videos of 300 frames (170 real sequences and 85 mask attacks), and as many 3D sequences with the corresponding depth information. Such a diversity of data permits a great flexibility for research in the field of face security to direct attacks, as it gives the possibility to study both 2D and 3D spoofing and anti-spoofing, and how these techniques could be potentially combined to increase the robustness of automatic face recognition systems to this type of threat.

## 3.3. Experimental protocol for 3D face spoofing attacks

The experimental protocol has been designed to fulfill the main objective set in the present work, that is, determine the risk posed by low-cost self-manufactured mask attacks to 3D and 2.5D face recognition technology. In order to report as unbiased and meaningful results as possible the protocol includes:

- *Data*. The new 3D-Face Spoofing Database (3DFSDB), which contains 3D, 2.5D and 2D real and spoof ing data that allow to perform a very wide range of different tests, including real performance evaluations and vulnerability spoofing assessment of 2D, 2.5D and 3D face recognition technology.
- *Systems*. Three different systems which include a commercial 3D solution and two proprietary implementations for 2.5D and 3D face recognition.
- *Experiments*. In order to fully characterize the risk posed by the mask attacks contained in the newly acquired 3DFS-DB, two performance evaluations under two different scenarios are carried out:

    *i*) Performance evaluation under the licit operation scenario; and

    *ii*) Performance evaluation under the spoofing attack scenario.

All these three elements, database, systems and experiments, are described in the next subsections. Then, results are presented in Section 3.4.

### 3.3.1. The JRC 3DFS Database

The new 3D Face Spoofing Database (3DFS-DB) has been constructed in order to comply with the requirements set for the experiments, that is: self-manufactured models using low-cost technology for 2D, 2.5D and 3D spoofing. The database is gender-balanced and contains real and fake facial data of 26 subjects, 13 men and 13 women, all Caucasian between 25 and 55 years of age.

The 3DFS-DB is composed of two datasets of real (3DFS-REAL) and fake (3DFS-FAKE) data. Each dataset contains: *i*) videos in *.avi* format for which both the 2D and 2.5D information is available; and *ii*) 3D models in *.stl* format. These data were acquired using two standard 3D scanners with a price of

around 200$: the Microsoft Kinect[15] and the PrimeSense Carmine 1.09[16]. This is the first face spoofing database acquired with two different sensors, which allows performing interoperability experiments.

Both sensors contain a standard RGB camera that captures 2D 640×480 pixel color data and an infrared projection system which detects the depth in the picture (i.e., 2.5D data). Both sensors incorporate the Light Coding technology developed by the Israeli based company Prime- Sense (recently acquired by Apple), however, the Carmine 1.09 scanner has a shorter range of operation (between 0.3-1.5 meters with respect to 0.8-4 meters of the Kinect) which enables it to achieve a maximum depth resolution of around 0.5 mm compared to the 1 mm resolution of Kinect.

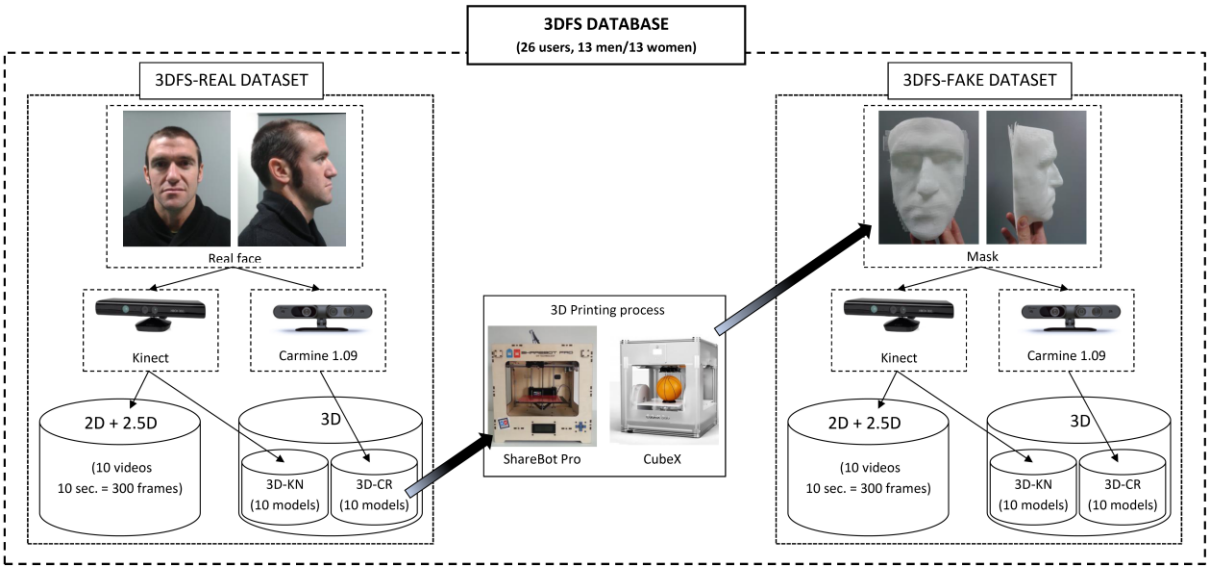


**Figure 5: General diagram of the structure and generation process of the new 3DFS-DB.**

Both datasets, real and fake, were acquired in an office like scenario with no specific illumination control and no constraints on the background except that no moving object was allowed.

Before the acquisition of the real dataset (3DFS-REAL) all invited users where informed of the nature of the experiments and the processing of their data with a privacy notice and signed a written consent form (please see Annex A) in compliance with the data protection legislative framework applied to EU institutions[17]. The processing operation of the experiment involving personal data has been the subject of a notification to the Data Protection Officer of the European Commission[18].

The enrolment procedure was conducted as follows:

- Videos: The user sat in front of the sensor and 10 second videos were acquired at a rate of 30 frames per second (i.e., 300 frames per video). Only small movements were

[15] http://en.wikipedia.org/wiki/Kinect

[16] http://en.wikipedia.org/wiki/PrimeSense

[17] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

[18] DPO-3702.2 - JRC : *Evaluation of Biometric Techniques at JRC/IPSC Institute: 3D Face and Fingerprint Recognition Spoofing*.

allowed during the video (i.e., blinking, breathing, slight head movements, etc.) and a pause of around one minute was left between videos. For each video both the 2D color data (640×480 pixel resolution) and the 2.5D depth information (640×480 pixel resolution and 1mm depth resolution) were captured simultaneously. Videos were acquired using only the Microsoft Kinect scanner.

- 3D models: The user sat in front of the sensor on a revolving chair and rotated at a regular speed 180$^{o}$ from left to right. The 3D models were acquired using the 90$ license application Skanect[19] and saved in *.stl* format. For each user five models were acquired with Kinect and five models with Carmine 1.09.

At the end of the real acquisition process users were also registered in the commercial application LogOn from ArtecID for securing computer access using the Carmine 1.09 sensor (see Section 3.3.2 for further details). As explained later, this is a black-box type application that does not allow having access to the enrolled features and, therefore, it is just used for testing purposes and these data is not released with the rest of the database.

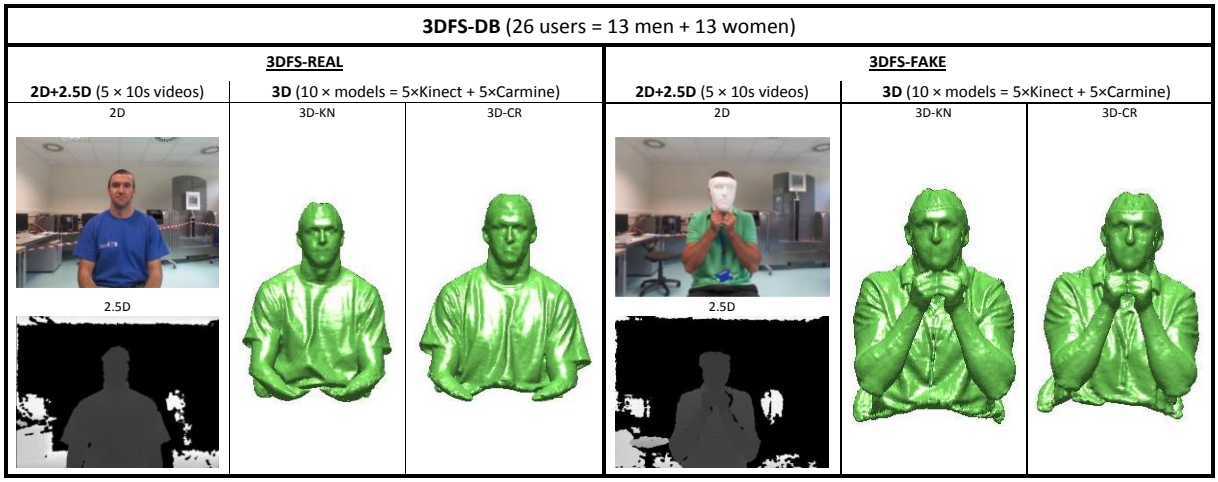


**Figure 6: Typical data samples that may be found in the 3DFS-DB. KN stands for data acquired with the Kinect scanner while CR stands for data acquired with the Carmine 1.09 scanner. See Section 3.3.1 and Figure 5 for further details about the structure and acquisition of the database.**

Once the 3DFS-REAL dataset was completed, the first 3D model of each user captured with the Carmine 1.09 scanner was processed (as later described in Section 3.3.2) and used to print one real size 3D reproduction of the subject's face. For this purpose two 3D printers were used, the ShareBot Pro[20] and the CubeX[21], worth around 1,000 and 2,000 euros, respectively. Half of the 26 models were generated with each of the printers. ABS plastic material was used to generate the physical artefacts as it resulted in better reproductions of the original models. The replicas were printed in natural size as, contrary to 2D recognition systems, 2.5D and 3D based algorithms are capable of detecting the real dimensions of objects and therefore are robust to miniaturized reproductions [109].

[19] www.skanect.com
[20] www.sharebot.it
[21] www.cubify.com

In a subsequent stage, the 26 fake models were acquired to generate the 3DFS-FAKE dataset. The acquisition methodology and scenario were the same as the ones described for 3DFS-REAL except that, in this case, the attacker would hold in front of his face the victim's face model.

Therefore, for each user, the database contains: 10 real and 10 fake videos (all captured with Kinect), and 10 real and 10 fake 3D models (5 captured with Kinect and 5 with Carmine 1.09). The general structure and generation process of the database is depicted in Figure 5, while some typical examples of the different data that may be found in each of the datasets are shown in Figure 6.

In Table 5 we give a comparative overview of the main characteristics of the new 3DFS database and the two other existing databases in the state of the art containing mask attacks spoofing data.

| | **COMPARATIVE SUMMARY: MASK-ATTACKS FACE SPOOFING DBs** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Overall Info. (Real/Fake)** | | | | **Sensor Info.** | | | **Attack (types)** | | |
| | **#IDs** | **# Samp** | **Videos** | **3D models** | **#** | **SQ** | **HQ** | **2D** | **2.5D** | **3D** |
| 3DFS DB | 26/26 | 780/780 | 260/260 | 520/520 | 2 | X | X | X | X | X |
| EURECOM MASK-ATTACK DB [21] | 20/16 | 200/160 | | 200/160 | 1 | | X | X | X | X |
| IDIAP MASK-ATTACK DB [20] | 17/17 | 170/85 | 170/85 | | 1 | X | | X | X | |

**Table 5: Comparative summary of the most relevant features corresponding to the new 3DFS-DB presented here, and the two previously existing 3D face spoofing databases considering mask attacks. # indicates number, Samp stands for samples, SQ for Standard Quality, and HQ for High Quality.**

### 3.3.2. Face Recognition Systems

Bear in mind that the objective of the work is not to develop new and more accurate face recognition systems, but to evaluate their robustness to self-performed mask attacks. For this purpose, three different state of the art systems were considered in the experiments:

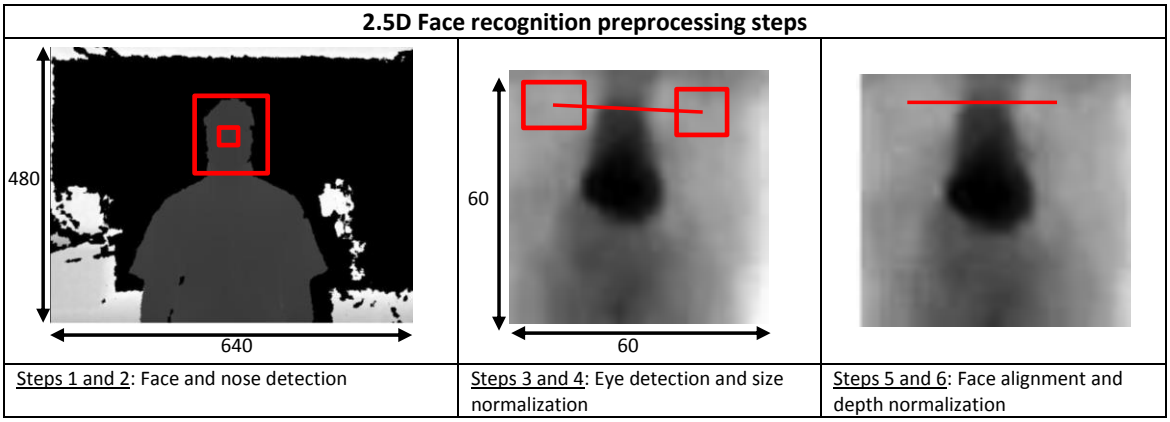


**Figure 7: Different preprocessing steps, prior to the similarity score computation, performed by the proprietary 2.5D face recognition system used in the experiments.**

- **2.5D Proprietary implementation**. The processing steps performed prior to the comparison of two 2.5D images are as follows: 1) face detection; 2) nose tip detection; 3) face segmentation and resizing to 60×60 pixels, forcing the nose tip to be in the center of the

image; 4) eye detection; 5 face alignment rotating the image to force the line that connects the eyes to be horizontal; 6) depth normalization forcing the nose tip (i.e., closest point of the size-normalized face to the sensor) to a 0 depth value. An example of the above mentioned processing steps is given in Figure 7. Finally, the similarity score between two normalized 2.5D faces is computed as the average Euclidean distance between all the pixels.

- **3D Proprietary implementation**. The system carries out the next preprocessing steps before computing the similarity scores between two 3D models: 1) head detection; 2) head segmentation from the rest of the body; 3) head rotation so that the eyes are aligned with the *x* axis; 4) face segmentation from the rest of the head; 5) face normalization forcing the nose tip to be at point (0*;* 0*;* 0). An example of the different processing steps is given in Figure 8. The similarity score between two normalized 3D face models is computed as the Hausdorff distance [193], [194], which measures how far two subsets (not necessarily composed of the same number of points) are from each other within a given metric space (in our case a three-dimensional space). In brief, two sets are close according to the Hausdorff distance if every point of either set is close to some point of the other set. The Hausdorff metric had already been successfully used in previous works to compare 2D images [195], 3D meshes [196], and in 3D face recognition [197].

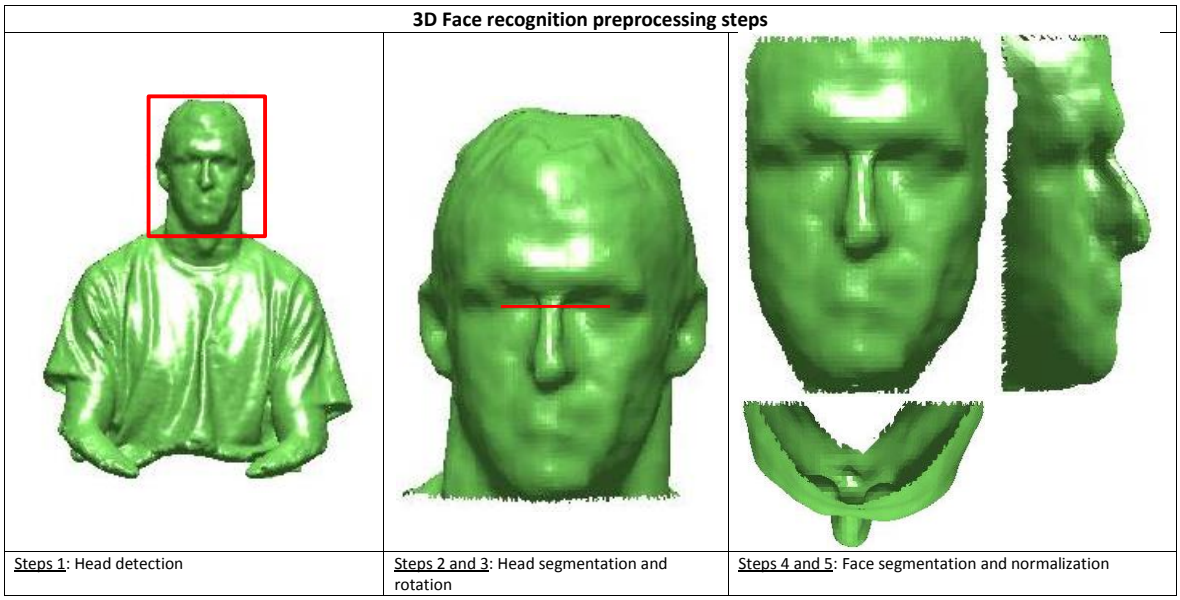


**Figure 8: Different processing steps, prior to the similarity score computation, performed by the proprietary 3D face recognition system used in the experiments.**

- **3D Commercial**: ArtecID 3D Face LogOn. This is a 3D face recognition system commercialized by ArtecID[22] which is designed to be integrated primarily on PCs and laptops as a method to securely sign-in in environments where restricted access is required such as financial, governmental, medical or forensic applications [198]. The software may work both on verification and identification modes and is specifically built to be compatible with the PrimeSense Carmine 1.09 sensor. Being a commercial product it is sold as a black box and no

[22] http://www.artecid.com/

specifications about the algorithms running inside are given. As score it outputs a similarity percentage (i.e., ranging from 0 to 100) between the enrolled model and the test sample.

Some typical real and fake processed 2.5D images and 3D models are shown in Figure 9. These are the type of processed samples used by the self-developed recognition systems described above for authentication purposes. A great similarity may be observed between both types of data, real and fake, illustrating the challenge posed by the mask attack described in the current contribution.

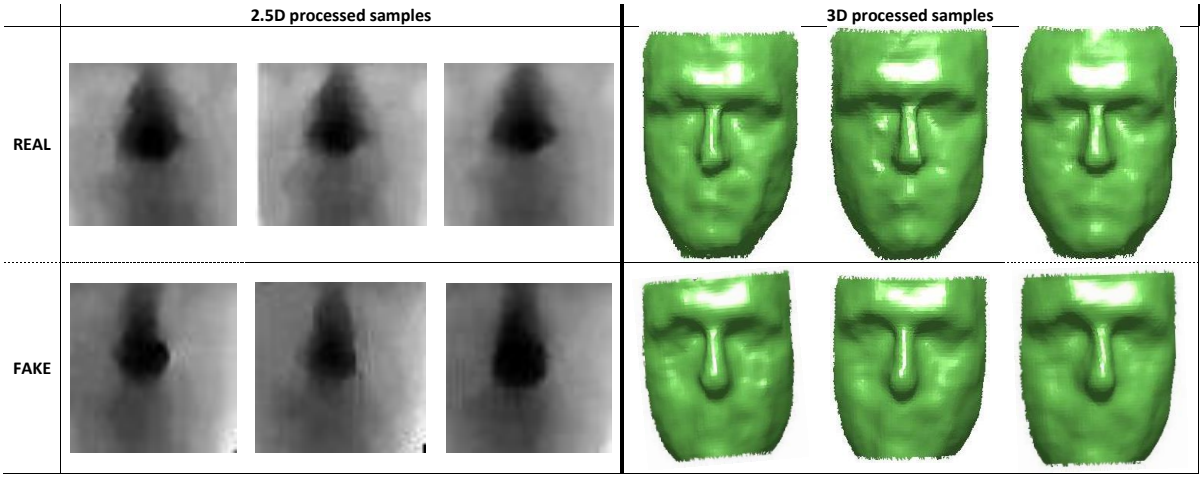


**Figure 9: Real and fake examples of 2.5D and 3D processed data generated by the self-developed recognition systems for authentication purposes.**

### 3.3.3. Experiments

Defining a clear methodology and its associated metrics to assess the "spoofability" of biometric systems is not a straight forward problem, as there are different variables and evaluations involved when the spoofing dimension is introduced. Although it is not yet generally deployed, an evaluation protocol which is gaining popularity for the assessment of biometric spoofing, defines two possible working scenarios [182], [80], [164], [107]:

- **Licit scenario**, considered in classic performance evaluations, it only takes into account genuine access attempts (i.e., regular access attempt in which a user logs in as himself) and zero-effort impostor access attempts (i.e., access attempts in which the attacker uses his own real biometric trait but claims to be a different user). In this scenario performance is typically reported in terms of the FRR (False Rejection Rate, number of genuine access attempts wrongly rejected) and the FAR (False Acceptance Rate, number of zero-effort impostor access attempts wrongly accepted). The working point where both the FRR and the FAR take the same value is the Equal Error Rate (EER).
- **Spoofing scenario**, where access attempts are either genuine (defined as before) or spoofing attacks where the intruder uses a physical artefact (in our case a 3D printed model) to impersonate the original user. Although for this last scenario there is still no agreed and standard way of reporting results, two metrics which have been proposed and are starting to be widely used are the FRR (defined as in the licit scenario) and the SFAR (Spoofing False Acceptance Rate, corresponding to the number of spoofing attacks wrongly accepted). The

working point where the FRR is equal to the SFAR is referred to in this work as the Spoofing Equeal Error Rate (SEER).

All these metrics (i.e., FRR, FAR and SFAR) should be strictly assessed to determine the real threat posed by a given spoofing database to a certain recognition system, as they allow to objectively determine the performance loss experimented between the two scenarios.

For each of the systems considered in the experiments and described in Section 3.3.2, the three sets of scores (i.e., genuine scores, zero-effort impostor scores and spoofing impostor scores) required to obtain the FRR, FAR and SFAR, were computed as follows:

- *2.5D proprietary system*. Each user was enrolled using five equally spaced processed frames from his first video. The remaining four real videos were used for testing, and for each of them five equally spaced processed frames were selected, totaling 40 test images per user. *Genuine scores* were computed comparing each of the 40 test samples to the five enrolled images of the same user, being the final score the average of the five partial scores between the test sample and the enrolled images. Therefore, a total 26×40=1040 genuine scores were generated. *Zero-effort impostor scores* were computed matching 5 randomly selected test samples of the remaining 25 users to the enrolled images of the user at hand, giving a total of 26×25×5=3250 zero-effort impostor scores. Finally, to compute the *spoofing impostor scores* all five fake videos were used for testing and five equally spaced frames were selected from each of them. Then, spoofing impostor scores were computed matching all 50 test spoofing samples of a given user to the five enrolled images of that same subject, resulting in 26×50=1300 spoofing impostor scores.
- *3D proprietary system*. The same protocol was used for the models produced with the Kinect and the Carmine 1.09 sensors. *Genuine scores* were computed using successively all five processed 3D face models for enrollment, and testing with the remaining four models avoiding repetitions, leading this way to 26×10=260 genuine scores. *Zero-effort impostor scores* were computed matching the first model from the 25 remaining users to the first model of a given subject, that is, 26×25=650 zero-effort impostor scores. *Spoofing impostor scores* were generated matching all five fake samples of the user to all five real models, resulting in 26×5×5=650 spoofing impostor scores.
- *3D Commercial: ArtecID 3D Face LogOn*. As this is a black-box type of system it allows for less flexibility than the previous two algorithms. All 26 users were enrolled to the system. To compute the *genuine scores*, each of them was asked to access his account five times, giving 26×5 = 130 genuine scores. To generate the *zero-effort impostor scores*, each user was asked to try to access the accounts of five different subjects, leading to 26×5=130 zero-effort impostor scores. Finally, *spoofing impostor scores* were computed using the fake reproductions to try to access five times the account of the genuine user, obtaining again 26×5=130 spoofing impostor scores.

## 3.4. Results

The experimental protocol described in Section 3.3 allows to objectively compare the performance of 2.5D and 3D face recognition systems in the licit and spoofing scenarios and, therefore, to fully characterize the risk posed by the studied self-manufactured low-cost mask attacks.

The distributions of the three sets of scores, genuine, zero-effort impostor and spoofing impostor, for each of the systems considered in the experiments are shown in Figure 10. In the case of the 3D proprietary system two different charts are presented, one for each of the sensors used to acquire the 3D models (Kinect and Carmine 1.09). It may be observed that the spoofing impostor attempts distribution is closer to the genuine scores than that from the zero-effort accesses, which means that the fake reproductions are more prone to be mistaken with the real users and, therefore, to break the systems.

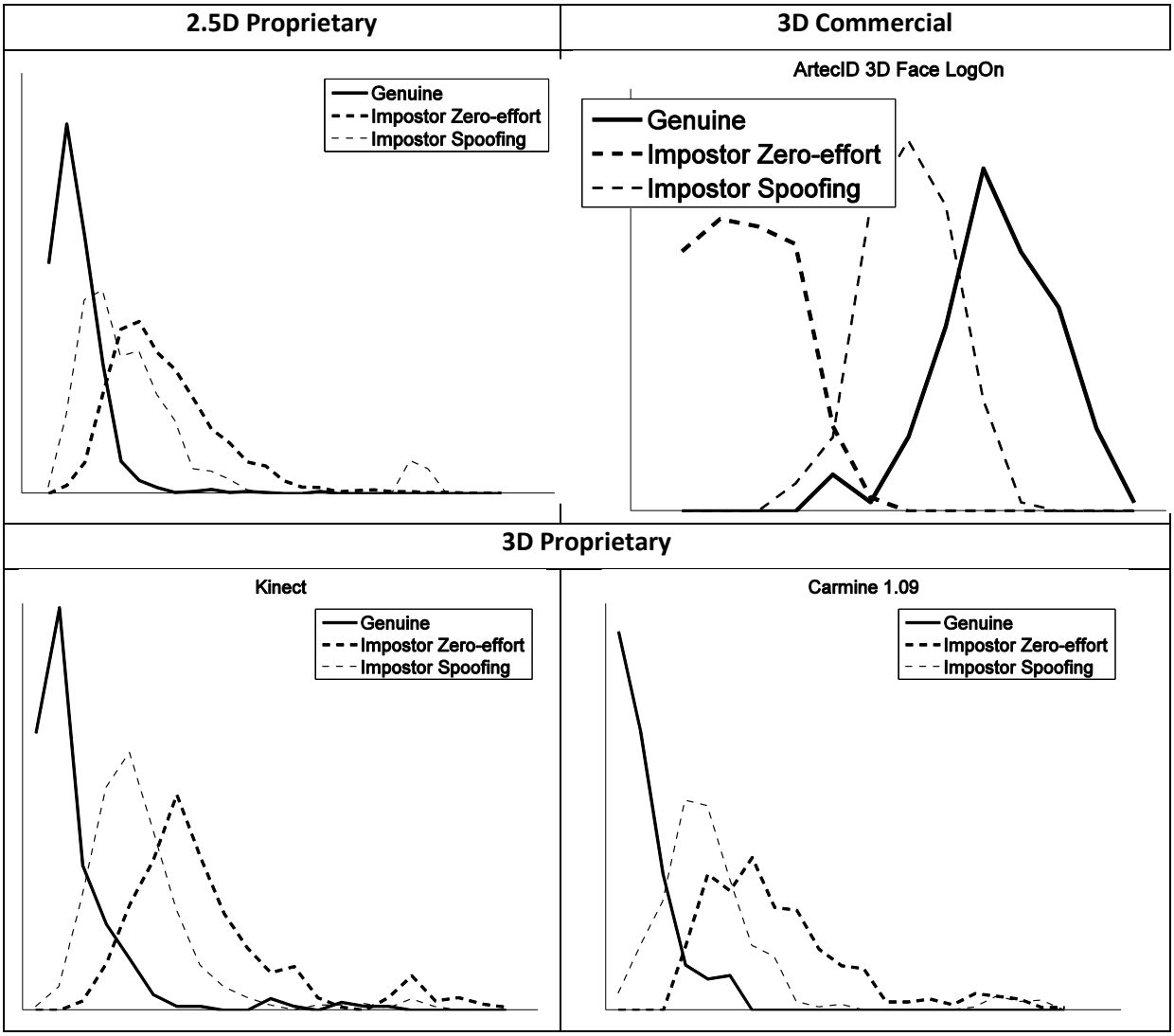


**Figure 10: Distributions of the genuine, zero-effort impostor and spoofing impostor sets of scores, for the three systems considered in the experiments. In the case of the proprietary 3D recognition system the sets of scores are computed for the two sensors used in the acquisition, Kinect and Carmine 1.09.**

These sets of scores are used to compute the metrics FRR-FAR in the licit scenario and FRR-SFAR in the spoofing case. Each of these two metric tuples are plotted in the form of Detection Error Trade-off (DET) curves in Figure 11, so that the performance of the systems may be visually compared in the two working scenarios considered. For each of the charts, the *x* axis represents either the FAR or the SFAR depending on the scenario selected (licit or spoofing). A quantitative comparison between the two scenarios may be obtained from the EER and SEER shown in the charts

legend. As in the case of the score distributions, two different curves are presented for the proprietary 3D face recognition system, one for each sensor used in the acquisition. Several interesting conclusions may be extracted from the results shown in Figure 10 and Figure 11:

- Regarding the licit scenario results, it may be observed that the performance of the proprietary systems considered in the work, based only on the face geometry/ shape, is still a step behind that of top-ranked 2D face recognition systems under good acquisition conditions (i.e., controlled illumination, pose and background). This corroborates the results obtained in past independent competitions [199], and shows that, in spite of the obvious advances in terms of size and price, off-the- shelf 3D sensing technology still needs to improve its accuracy to reach really competitive recognition results in the field of face authentication.
- Also worth noting that, in the licit scenario, the higher resolution of the Carmine 1.09 sensor with respect to Kinect translates into better performance, decreasing the EER from 12.5% to 10.5%.
- Interestingly, the 2.5D recognition system reaches a higher accuracy (EER=7.5%) than the system based on the complete 3D model of the face (EER=10.5%). This may be explained by the fact that, in the experiments, the 2.5D algorithm uses five images for enrolment and averages all five scores obtained from the matching to the test image, while the 3D system considers only one enrolled model. Therefore, a direct comparison between the performance of both systems is difficult to be established.
- In the spoofing scenario, the proprietary 3D system shows a higher resilience to the attack than the 2.5D algorithm which presents a SEER of almost 50%. This result reinforces the idea that it is more difficult to reproduce the exact geometry of the whole face than just the depth map of a 2D image.
- Overall, the results depicted in Figure 10 and Figure 11 show the high vulnerability of all tested systems, even the commercial solution, to the proposed attack. On average, there is an increase of around 210% between the EER and the SEER of the different algorithms evaluated.

## 3.5. Conclusions of the JRC case study

Face recognition systems based on 3D data are robust to classical spoofing attacks typically carried out with 2D surfaces such as printed photographs or screens of portable devices. However, 3D face recognition technology may fail the challenge posed by more sophisticated type of attacks based on the presentation of a face reproduction to the acquisition sensor.

This work has presented the first vulnerability evaluation of 2.5D and 3D face recognition systems to spoofing attacks performed with low-cost self-manufactured face models. Experiments have been carried out on a new database, the biggest of this type acquired to date (i.e., considering 3D face spoofing attacks), which will be made available for researchers. Results have been obtained following fully reproducible protocol and they have been reported based on metrics which, in the absence of a standardized way of assessing biometric “spoofability”, are the most widely used methodology to present the outcome of a spoofing study in a meaningful and usable way.

Although the statistical significance of the study is limited due to the relatively small amount of data considered (i.e., 26 subjects), we believe that, from a qualitative point of view, the results show

the high vulnerability of the assessed systems, including the commercial solution evaluated, to this type of threat. Even if results could vary from a quantitative perspective on a larger database, the work may still be seen as a consistent and reliable proof of concept of the studied attack.

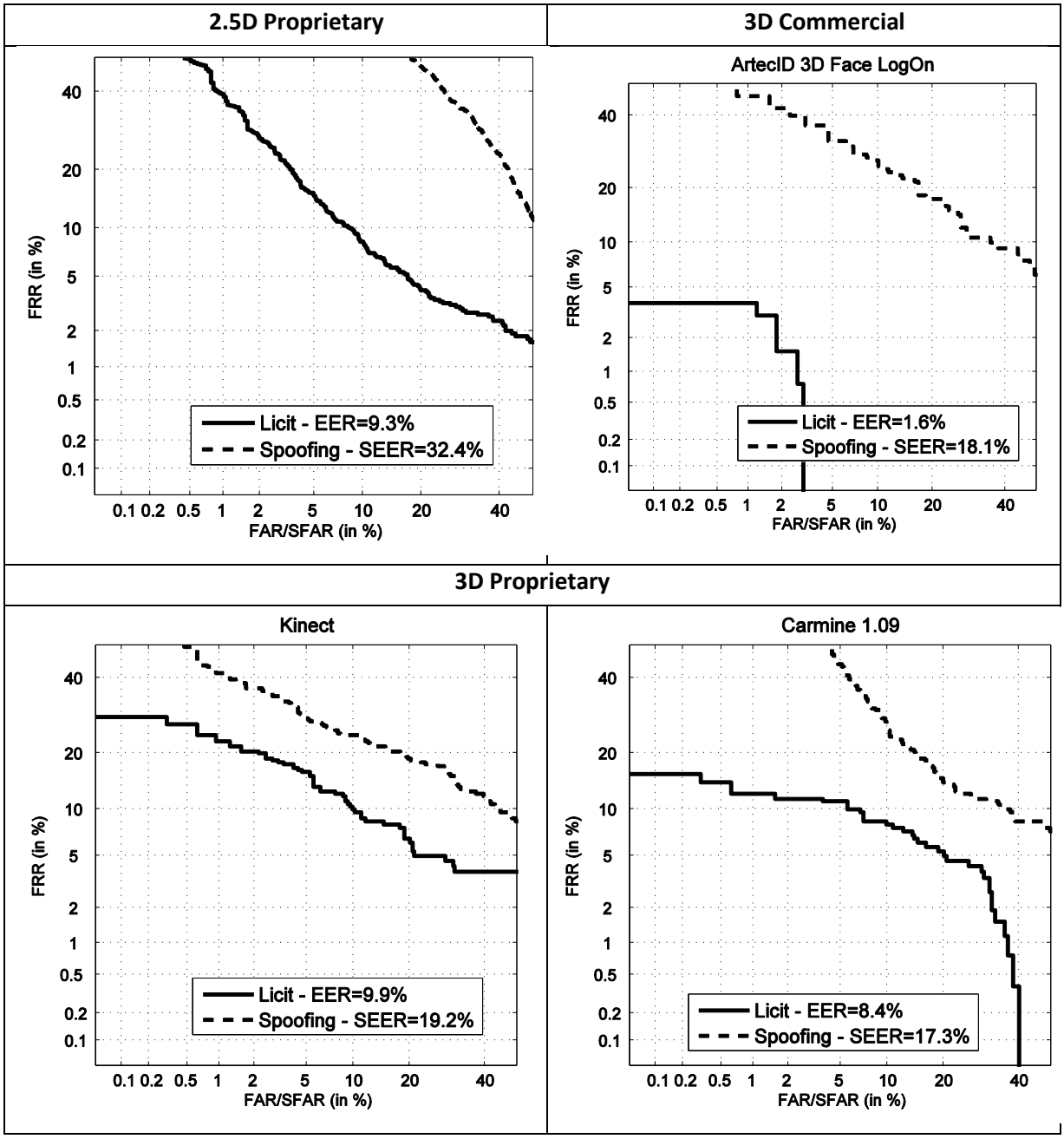


**Figure 11: DET curves for the two considered scenarios, licit and spoofing, and for the three systems used in the experiments. The x axis shows the FAR or the SFAR depending on the scenario. Two charts are shown for the proprietary 3D face recognition system, one for each sensor used in the acquisition.**

The risk posed by the attacks is even greater considering the "do-it-yourself" nature of the study, which makes them accessible to the general public with no intervention from third parties and with a very limited budget. Therefore, the work has raised the need to develop adequate countermeasures against this potential security breach.

The work has been designed and developed applying the *security through transparency principle* largely followed by industry, researchers and vendors, to analyze biometric security from the initial steps of this technology. This principle was first formulated in the field of cryptography and then generalized to all other security areas as *"the enemy knows your system"* [200]. It states that the fewer and simpler the things one needs to keep secret in order to ensure the security of a given system, the easier it is to maintain that security. In other words, there is no point in trying to deny or cover the vulnerabilities of biometric systems to spoofing because, sooner or later, attackers will discover them and the consequences will be unpredictable [179]. Therefore, quoting the Biometric Working Group position already in year 2003: "*public exposure of countermeasures and vulnerabilities will lead to a more mature and responsible attitude from the biometrics community and promote the development of more secure systems in the future*" [180].

In summary, the current case study may be understood as a consistent and rigorous practical example which shows that, although a great amount of work has been done and many advances have been reached in the field of spoofing detection, attacking methodologies have also evolved and become more and more sophisticated as a direct consequence of the permanent technological progress. This way, there are still big challenges to be faced in the protection against spoofing, that will hopefully lead in the coming years to a whole new generation of more secure biometric systems.

# 4. Summary and discussion: Lessons, facts and challenges

In “Skyfall”, the latest movie in the James Bond saga, 007 is given a gun that only he can fire: It works by recognizing his palmprint, rendering it useless when it falls into a baddy’s hands. This is just another example of the multiple uses which have been given to biometrics in films, TV and books, in most cases assuming a zero-error and perfect security performance.

However, as usually happens in terms of technical advances, reality is still some distance away from fiction: *“On September 2013, the world witnessed a long anticipated event, heralding a paradigm shift in mobile security: Apple’s launch of the new iPhone 5S with a fingerprint reader underneath the home button. The use case: to unlock the phone and authorize purchases in Apple’s iStore. One day after the iPhone hit the shelves, a hacker team claimed to have circumvented the biometric system through getting the phone to accept a fake ‘spoofed’ fingerprint.”*[177]

A great amount of research has been carried out concerning the vulnerabilities of biometric systems to direct attacks and multiple techniques to secure them against this threat have been proposed. Moreover, as it has been shown in different independent evaluations, some of these protection techniques present very competitive results, in some cases close to 100% accuracy, when they are assessed in laboratory conditions. However, in spite of all these efforts, commercial products, even those developed by the most advanced technological companies, keep failing to withstand the challenges posed by hackers. How can this situation be explained? Like in most cases, a simple answer is not possible as a number of factors have contributed to reach the current status.

From the experience gained from the thorough review of the general state of the art in spoofing presented in this report (see Sect. 2) and from the case study conducted at the JRC on 3D face spoofing (see Sect. 3), in our view there are several needs and challenges that still need to be addressed in this field:

### *Need for a certification methodology*

Although some efforts have been made in the frame of the Common Criteria [41], [181] and there is on-going work to release the first ISO standard specifically focused on spoofing [42], still no largely extended standard exists regarding the evaluation of biometric vulnerabilities. This has resulted in very sparse certifications of biometric-based security commercial products compared to other technologies with a long standardization trajectory such as smart cards or cryptography [45], [46], [47]. A clear and well defined certification methodology to assess biometric security capabilities would certainly help vendors and developers in their work of designing more robust and reliable systems.

### *Need for an evaluation methodology of anti-spoofing measures*

So far, biometric spoofing questions have been addressed by the research community mainly relying on empirical testing carried out by individual research groups to demonstrate and compare performances of some specific techniques, often with a small-scale dataset put together in an ad-hoc way. Although this learn-by-doing approach permits to gain some insight into the new problem at hand, in the field of direct attacks there is still not enough understanding of how to quantitatively

address performance tradeoffs and limits as there is still no established and sound spoofing evaluation methodology.

Developing a methodology to assess the "spoofability" of systems is not a straight forward problem, as there are different variables and evaluations involved when the spoofing dimension is introduced. Although it is not yet generally deployed, the evaluation protocol followed in the case study and described in the present report (see Section 3.3) is gaining popularity and should be the subject of further developments.

The different metrics involved in this evaluation methodology (i.e., FRR, FAR and SFAR) should be strictly assessed before carrying out any further evaluation concerning liveness detection techniques. This way, the real threat posed by the spoofing database to a certain recognition system can be determined. Then, if a countermeasure is introduced in the system, a rigorous evaluation should re-compute all three previous measures (i.e., FRR, FAR and SFAR) considering the anti-spoofing module, so that they can be compared to the case with no protection against direct attacks. Thereby, the real impact of the liveness detection technique on the system under the two possible operating scenarios (i.e., licit and spoofing) is fully characterized.

Currently, when it comes to the evaluation of a new anti-spoofing countermeasure, in most cases, its performance is measured as an independent module and reported in terms of its classification rates, usually referred to as FFR (False Fake Rate, number of real samples classified as fake) and FLR (False Living Rate, number of fake samples classified as real). This stand-alone assessment constitutes a first necessary step towards the evaluation of the countermeasure but, as specified above, it should be complemented with further analyses. In fact, a liveness detection algorithm will, in general, not function on its own but integrated in a recognition system. In this framework, to perform an exhaustive assessment, other questions which are very rarely answered in current state-of-the-art works, should be addressed:

- What is the impact of the FFR and FLR on the system performance (i.e., FRR, FAR and SFAR)?
- On the other hand, how can the similarity scores be combined with the anti-spoofing module to improve the robustness of the whole system against direct attacks?

Although the above methodology would already represent a big advance if it was widely adopted or implemented into a standard, it still opens some new interesting topics for research which have just started to be explored:

- What is the best way to combine matching and liveness-detection scores [184], [164]?
- What would be the impact of this fusion in multibiometric systems [182]?
- Can the performance of a system under both operating scenarios (i.e., licit and spoofing) be reported with one single metric?
- How can the above two-scenario methodology be generalized to the real case where all three score classes (i.e., genuine, zero-effort and spoofing) are present at the same time?

Even if these preliminary efforts in the study of spoofing assessment principles are hugely valuable, there is still a quite limited theoretical foundation in this field to be able to answer some of the fundamental questions listed above. Accordingly, the biometric community needs to confront the existing challenges in order to build a solid theoretical background that allows the further development of this area.

### *Need for realistic evaluation conditions*

A consistent evaluation methodology would be of limited use if it is not developed under the correct context. It is especially challenging to recreate real attacking conditions in a laboratory evaluation. Under controlled conditions, systems are tested against a restricted number of typical spoofing artefacts, as it is unfeasible to collect a database with all the different possibilities that may be found in the market. Furthermore, assessment databases are usually divided into train and test sets in which both of them contain examples of the same spoofs, therefore, the techniques can be specifically tuned on the train set to detect what they already know will be present in the test set. However, the real world represents an open set evaluation. In this scenario, what can be expected from the performance of the protection technique against *any* type of spoof and not only those for which it has been trained?

### *Need for interoperable algorithms*

To date, the competitions organised have shown that top-ranked algorithms are able to achieve an accuracy close to 100%, however, their performance drops significantly when the testing dataset is changed. An interesting lesson may be learned from these results: There exists no clear superior anti-spoofing technique, as this will depend on the nature of the attack scenarios and acquisition conditions. Therefore, it is important to find complementary countermeasures and study the best fusion approaches in order to develop liveness-detection techniques that generalize well to different spoofing data [165], [185].

### *Need for further fundamental biological-related research*

The anti-spoofing community should also consider engaging in new fundamental research regarding the biological dimension of biometric traits, in order to break with the current popular trend embraced by many of the latest research where some well-known sets of features (e.g, LBP, LPQ, HOG or BSIF) are extracted from the images of public databases and passed through a classifier. Although such a methodology is valid, in most cases it brings little new insight into the spoofing problem. A greater progress could potentially be obtained from new studies exploiting intrinsic biological differences between real and fake traits such as, for instance, the thermogram or the amount of facial blood flow.

New technology and hardware-based advances can greatly help in this biological-related research line. As technology progresses, new devices and sensors continue to emerge. It is important to keep track of this rapid progress since some of the new sensing technologies can be the key to develop novel and efficient anti-spoofing techniques. For example, just a few years ago, 3D acquisition scanners were unsuitable for liveness detection purposes due to their cost, size and level of cooperation required from the user. However, nowadays, there exist sensors which provide accurate depth information, with the size of a regular webcam and almost for its same price. Should they become integrated in biometric readers, such sensors could become in the near future a definitive solution against 2D photo and video attacks to face and iris. Although, as shown in the present work, their potential efficiency against 3D mask attacks is at least questionable.

### *Need for spoofing related studies in forensics*

The impact of spoofing should also be considered in other biometric-related fields such as forensics. Sir Arthur Conan Doyle already foresaw the possibility of fake fingerprint forensic evidence

in one of his renowned Sherlock Holme's short stories over a century ago [186]. Since then, different works have tested the ability of forensic examiners to distinguish between real and fake latent fingerprints [187], [188]. However, only recently have some interesting research works addressed the *automatic* detection of fake finger-marks deliberately left behind at crime scenes [189], [190], [191]. This is a research line that can gain a lot of strength and importance in the years to come.

### *Need for a balance between security and convenience*

Another question to be addressed in the field of spoofing, is the balance between security and convenience. It is undeniable that one of the most important motivations, if not *the* most important reason, for the deployment and development of biometrics, is its security dimension. We want to secure access to information and biometrics represents a good alternative: you are your own key. In this context, spoofing gains great relevance: if the system is spoofed, the information is compromised.

However, it is important to keep in mind the final product where the biometric system will be integrated and its ultimate purpose within that product, as security is just one side of the coin. The other side is convenience. For certain applications, from the end-user perspective, some risk of spoofability may be acceptable if, in return, he obtains a greater gain in convenience.

For instance, before the appearance of the iPhone 5S it was estimated that over 50% of users had not set any security mechanism to unlock their mobile phones before the introduction by apple of the *convenient* fingerprint reader. If such percentage is decreased with the use of biometrics, it may be argued that a convenient and spoofable system has increased the overall security of mobile phones.

### *Next steps at the JRC*

Regarding the 3D face spoofing evaluation conducted at the JRC, it has shown the lack of robustness of this technology against direct attacks and the need to develop and integrate new protection measures. As such, and given also the needs and challenges expressed above in the spoofing field, the next steps that are foreseen within the BBM project in the JRC G.06 unit will be focused on the proposal and systematic evaluation of novel anti-spoofing techniques for face 3D-base recognition systems:

- Research on new hardware-based countermeasures to 3D face spoofing attacks. Such techniques will be based on new sensing technology for intrinsic biological signals such as the blood flow or corporal temperature.
- Research on the fusion of 2D, 2.5D and 3D modalities to develop more robust overall systems.
- Proposal of new metrics that can help to reach a homogeneous and consistent anti-spoofing evaluation methodology.
- System-base evaluations of further face recognition 3D-based commercial solutions.

### *Wrap-up*

As a wrap up conclusion it may be stated that, although as shown in the present report, a great amount of work has been done in the field of spoofing detection and many advances have been reached, the attacking methodologies have also greatly evolved and become more and more sophisticated. As a consequence, there are still big challenges to be faced in the protection against direct attacks, that will hopefully lead in the coming years to a whole new generation of more secure biometric systems.

In the meanwhile, Mr Bond will still have to wait some time until he gets a gun that he can *fully trust* to be the only person who can fire it.

# Annex A. Data protection activities

In this Annex, we collect the different data protection documents and measures adopted for the acquisition and later post-processing of the JRC 3D-Face Spoofing Database described in Sect. 3.3.1, and used in the 3D face spoofing case study conducted by the JRC described in Sect. 3.3.

## A.1. Data acquisition privacy statement

Below the reader can find the consent form which was given in advance to the data acquisition campaign to all invited users. Users were entitled to any type of clarification prior to signing the document.

## PRIVACY STATEMENT

### Evaluation of Biometric Techniques at the JRC/IPSC Institute: 3D Face and Fingerprint Recognition Spoofing

**1. Description**

This processing of personal data is to conduct scientific and experimental research on the evaluation of biometric techniques used in access control identity recognition tasks for border management. A data collection will be organised on voluntary basis to investigate vulnerabilities of fingerprint recognition and 3D face recognition to spoofing attacks.

The evaluation of 3D spoofing with printed masks requires processing steps for capturing, recording, 3D printing, filing of 3D images, printed masks and user demographics (gender). The experimental test will focus on evaluating the technological maturity of commercial / open-source 3D sensing and printing techniques in producing realistic cheap 3D printed masks and assessing their use as threats to current 3D face recognition solutions. The results might also contribute to enhance novel access control procedures where 3D face recognition technology is already installed (e.g. airport access control for 2014 Winter Olympic Games in Sochi).

The evaluation of fingerprint vulnerabilities to spoofing attacks requires processing steps for capturing, recording, evaluating, and intelligently merging pairs of fingerprint geometrical/landmark features (i.e. two sets of fingerprint templates per individual) and user demographics (age and gender). The experimental tests will focus on identifying the technological specifications for higher resilience to spoofing attacks.

As a complementary and preliminary step of the previous point, factors affecting the quality of the fingerprint acquisition process will be analysed. In fingerprint based access control identity recognition tasks, image acquisition is the most crucial step as any information loss at this phase can hardly be recovered. To better quantify image quality effects and capturing conditions likely to impact on recognition accuracy of the latest capturing devices (e.g. multispectral, touchless readers), experimental tests need to be

conducted.

All acquired images will be processed to constitute a database of models of real faces, printed masks and fingerprint templates.

A testbed for 3D face spoofing with printed masks and fingerprint recognition will be implemented. Low cost software and capturing devices (i.e. off-the shelf 3D face/fingerprint recognition systems, 3D camera sensors, touchless/multispectral fingerprint readers and 3D printers) will be used by a specialised operator in a controlled environment.

Your personal data will be collected and further processed for the purposes detailed hereafter under point 2. The processing of personal data is under the responsibility of the Unit Head of the JRC/IPSC Digital Citizen Security Unit who acts as controller of this processing.

As this processing collects and further processes personal data, Regulation (EC) 45/2001, of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, is applicable.

**2. What personal information do we collect, what is the legal basis, for what purpose and through which technical means?**

**Identification Data:**

The personal data collected and further processed are:

- Scanned face for 3D models and printed masks (identifier, gender,

- Fingerprint templates extracted from images (500 dpi) of the two index fingers

- Identifier, age and gender of volunteers

**Legal Basis of processing:**

- COUNCIL DECISION of 19 December 2006 concerning the Specific Programme to be carried out by means of direct actions by the Joint Research Centre under the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2006/975/EC) (2007 to 2013)
- Horizon 2020 - The Framework Programme for Research and Innovation - Communication from the Commission.

The processing of personal data is lawful following Art. 5a

**Purpose of processing:**

The processing will evaluate biometric techniques used in access control identity recognition tasks (face and fingerprint features)

For face recognition assessment, the purpose of the processing is to evaluate current low cost/commercial 3D face recognition technology and its resilience to spoofing attacks with printed masks attacks.

For fingerprint recognition assessment, the purpose of the processing is to study the resilience of latest commercial fingerprint recognition technology to spoofing attacks generating universal mixed identifiers will be investigated. It will be complemented by the study of the acquisition dependent aspects affecting fingerprint recognition rate such as

physical aspects related to finger anatomy, physical conditions of the finger(s) (i.e. normal. Humidity, sugar, and dirt) and capturing devices, including latest touchless/multispectral sensors.

**Technical Information:**

The user data are collected through sensing and biometric devices (3D cameras and fingerprint readers), processed and stored in an encrypted database on G07 lab server, physically disconnected for JRC Intranet and not accessible from outside world.

**3. Who has access to your information and to whom is it disclosed?**

- Access to all personal data is only granted through User_Id / Password to a defined population of users. These users are: the Unit Head acting as controller of the processing of personal data and the four unit staff members from the Biometric and Border Management project in charge of this deliverable.

**4. How do we protect and safeguard your information?**

The collected personal data is stored on the servers of JRC and underlie the Commission Decision C (2006) 3602 of 17/08/2006 “concerning the security of information systems used by the European Commission” defines IT security measures in force. Annex I defines the security requirements of EC Information Systems. Annex II defines the different actors and their responsibilities. Annex III defines the rules applicable by users. See JRC corporate notification DPO-1946.

**5. How can you verify, modify or delete your information?**

In case you want to verify which personal data is stored on your behalf by the controller, please contact us by email at G07-secreteriat@jrc.ec.europa.eu.

Upon a justified request submitted to the above mentioned functional mailbox, your data will be rectified, modified, frozen or eventually erased in a maximum period of 14 days.

**6. How long do we keep your data?**

Your personal data is kept until the end of lifecycle of the processing:

Biometric and personal data will be retained in raw format for the time necessary to perform resilience to spoofing project (2 years).

**7. Contact Information.**

Should you have any queries concerning the processing of your personal data, please address them to the controller under the following mailbox:

. G07-secreteriat@jrc.ec.europa.eu

On questions relating to the protection of personal data, you can contact:

. - the DG JRC Data Protection Co-ordinator: jrc-data-protection-coordinator@ec.europa.eu

. - the Commission’s Data Protection Officer: data-protection-officer@ec.europa.eu

**8. Recourse.**

In the event of a dispute, you can send a complaint to:

- the European Data Protection Supervisor: edps@edps.europa.eu

☐ I consent to provide my fingerprints for the purpose of this project

☐ I do not consent to provide my fingerprints

☐ I consent to provide my 3D face scanned to the experiment

☐ I do not consent to provide my 3D face scanned

Date Signature for approval

## Bibliography


[1] W. W. Bledsoe, “The model method in facial recognition,” Panoramic Research Inc., Palo Alto, CA, Tech. Rep. PRI:15, 1964.

[2] M. D. Kelly, “Visual identification of people by computer,” Stanford AI Project, Stanford, CA, Tech. Rep. AI-130, 1970.

[3] K. H. Davis, R. Biddulph, and S. Balashek, “Automatic recognition of spoken digits,” *Journal of the Acoustical Society of America*, vol. 24, pp. 637–642, 1952.

[4] A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for information security,” *IEEE Trans. on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006.

[5] The Guardian, “iphone 5s fingerprint sensor hacked by germany’s chaos computer club,” Available on-line, 2013, http://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked.

[6] The Register, “Get your german interior minister’s fingerprint here,” Available on-line, 2008, http://www.theregister.co.uk/2008/03/30/german interior ministerfingerprint appropriated/.

[7] The CNN, “Man in disguise boards international flight,” Available on-line, 2010, http://edition.cnn.com/2010/WORLD/americas/11/04/canada.disguised.passenger/.

[8] PRA Laboratory, “Fingerprint spoofing challenge,” YouTube, 2013, http://www.youtube.com/watch?v=vr0FmvmWQmM.

[9] Discovery Channel, “Mythbusters: Fingerprints cannot be busted,” YouTube, 2011, http://www.youtube.com/watch?v=3Hji3kp-i9k.

[10] Chaos Computer Club Berlin, “Hacking iphone 5s touchid,” YouTube, 2013, http://www.youtube.com/watch?v=HM8b8d8kSNQ.

[11] Sky News, “Fake fingers fool hospital clock-in scanner,” Available on-line, 2013, http://news.sky.com/story/1063956/fake-fingers-fool-hospital-clockin-scanner.

[12] Tech Crunch, “Woman uses tape to trick biometric airport fingerprint scan,” 2009, http://techcrunch.com/2009/01/02/woman-uses-tape-to-trick-biometricairport-fingerprint-scan/.

[13] BBC News, “Malaysia car thieves steal finger,” Available on-line, 2005, http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.

[14] The Daily Mail, “The man in the latex mask,” Available on-line, 2012, http://www.dailymail.co.uk/news/article-2153346/Black-armed-robber-disguisedwhite-man-using-latex-mask.html.

[15] N. M. Duc and bui Quang Minh, “Your face is not your password: Face authentication bypassing lenovo-asus-toshiba,” in *Black Hat USA*, 2009.

[16] Tabula Rasa, “Tabula rasa spoofing challenge,” 2013, http://www.tabularasa-euproject.org/evaluations/tabula-rasa-spoofing-challenge-2013.

[17] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric recognition: security and privacy concerns,” *IEEE Security and Privacy*, vol. 1, pp. 33–42, 2003.

[18] R. Bolle, J. Connell, and N. Ratha, “Biometric perils and patches,” *Pattern Recognition*, vol. 35, pp. 2727–2738, 2002.

[19] A. Wehde and J. N. Beffel, “Fingerprints can be forged,” *Tremonia Publish Co.*, 1924.

[20] L. Thalheim and J. Krissler, “Body check: biometric access protection devices and their programs put to the test,” *ct magazine*, pp. 114–121, November 2002.

[21] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, “An evaluation of indirect attacks and countermeasures in fingerprint verification systems,” *Pattern Recognition Letters*, vol. 32, pp. 1643–1651, 2011.

[22] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, “On the vulnerability of face verification systems to hill-climbing attacks,” *Pattern Recognition*, vol. 43, pp. 1027–1038, 2010.

[23] P. Mohanty, S. sarkar, and R. Kasturi, “From scores to face templates: a model-based approach,” *Pattern Analysis and Machine Intelligence*, vol. 29, pp. 2065–2078, 2007.

[24] C. Rathgeb and A. Uhl, “Attacking iris recognition: An efficient hill-climbing technique,” in *Proc. Int. Conf. on Pattern Recognition (ICPR)*, 2010, pp. 1217–1220.

[25] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, vol. 579416, p. 17, 2008.

[26] B. Toth, “Biometric liveness detection,” *Information Security Bulletin*, vol. 10, pp. 291–297, 2005.

[27] K. Kollreider, H. Fronthaler, and J. Bigun, “Non-intrusive liveness detection by face images,” *Image and Vision Computing*, vol. 27, pp. 233–244, 2009.

[28] Z. Wei, X. Qiu, Z. Sun, and T. Tan, “Counterfeit iris detection based on texture analysis,” in *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, 2008.

[29] S. Marcel, M. Nixon, and S. Z. Li, Eds., *Handbook of Biometric Anti-Spoofing*. Springer, 2014.

[30] K. A. Nixon, V. Aimale, and R. K. Rowe, *Handbook of Biometrics*. Springer, 2008, ch. Spoof detection schemes, pp. 403-423.

[31] G. Pan, Z. Wu, and L. Sun, *Recent advances in face recognition*. Intech, 2008, ch. Liveness detection for face recognition, pp. 236–252.

[32] Z. Akhtar, “Security of multimodal biometric systems against spoof attacks,” Ph.D. dissertation, University of Cagliari, 2012.

[33] J. Galbally, “Vulnerabilities and attack protection in security systems based on biometric recognition,” Ph.D. dissertation, Universidad Autonoma de Madrid, 2009.

[34] E. Marasco, “Secure multibiometric systems,” Ph.D. dissertation, University of Naples Federico II, 2010.

[35] P. Coli, “Vitality detection in personal authentication systems using fingerprints,” Ph.D. dissertation, Universita di Cagliari, 2008.

[36] M. Sandstrom, “Liveness detection in fingerprint recognition systems,” Master’s thesis, Linkoping University, 2004.

[37] M. Lane and L. Lordan, “Practical techniques for defeating biometric devices,” Master’s thesis, Dublin City University, 2005.

[38] J. Blomme, “Evaluation of biometric security systems against artificial fingers,” Master’s thesis, Linkoping University, 2003.

[39] R. Derakhshani, “Determination of vitality from a non-invasive biomedical measurement for use in integrated biometric devices,” Master’s thesis, West Virginia University, 1999.

[40] *ISO/IEC 19792:2009, Information technology - Security Techniques - Security Evaluation of Biometrics.*, ISO/IEC Std., 2009.

[41] BEM, “Biometric Evaluation Methodology. v1.0,” 2002. IEEE ACCESS, VOL. XX, NO. XX, MONTH YEAR 19

[42] *ISO/IEC CD 30107-1. Information Technology - Biometrics - Presentation Attack Detection - Part 1: Framework*, ISO/IEC Std., 2016, under development.

[43] Centro Criptologico Nacional (CCN), “Characterizing attacks to fingerprint verification mechanisms CAFVM v3.0,” Common Criteria Portal, 2011.

[44] Bundesamt fur Sicherheit in der Informationstechnik (BSI), “Fingerprint spoof detection protection profile FSDPP v1.8,” Common Criteria Portal, 2008.

[45] Federal Office for Information Security, “Certification Report, BSI-DSZ-CC-0511-2008 for PalmSecure SDK Version 24 Premium from Fujitsu Limited,” Federal Office for Information Security, Tech. Rep., 2008.

[46] Centro Criptologico Nacional, “Certification report, 2009-30-INF-515 v1 for Authentest Server v1.2.6 from Authenware Corp.” Ministerio de Defensa de España, Tech. Rep., 2010.

[47] Federal Office for Information Security, “Certification Report, BSI-DSZ-CC-0790-2013 for MorphoSmart Optic 301, Version 1.0 from Safran Morpho,” Federal Office for Information Security, Tech. Rep., 2013.

[48] P. Lapsley, J. Less, D. Pare, and N. Hoffman, “Anti-fraud biometric sensor that accurately detects blood flow,” US Patent 5,737,439, 1998.

[49] E. Diaz-Santana and G. Parziale, “Liveness detection method,” US Patent EP1 872 719, 2008.

[50] J. Kim, H. Choi, and W. Lee, “Spoof detection method for touchless fingerprint acquisition apparatus,” Korea Patent 1 054 314, 2011.

[51] *International Joint Conference on Biometrics (IJCB)*. IEEE, 2011.

[52] *Int. Biometric Performance Testing Conference*. National Institute for Standards and Technology, 2012, http://www.nist.gov/itl/iad/ig/ibpc2012.cfm.

[53] *IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP)*. IEEE, 2013, http://www.icassp2013.com/SpecialSessions.asp.

[54] I. Chingovska, J. Yang, Z. Lei, D. Yi, S. Z. Li, O. Kahm, C. Glaser, N. Damer, A. Kuijper, A. Nouak, J. Komulainen, T. Pereira, S. Gupta, S. Khandelwal, S. Bansal, A. Rai, T. Krishna, D. Goyal, M. Waris, H. Zhang, I. Ahmad, S. Kiranyaz, M. Gabbouj, R. Tronci, M. Pili, N. Sirena, F. Roli, J. Galbally, J. Fierrez, A. Pinto, H. Pedrini, W. S. Schwartz, A. Rocha, A. Anjos, and S. Marcel, “The 2nd competition on counter measures to 2d face spoofing attacks,” in *Proc. IAPR Int. Conf. on Biometrics (ICB)*, 2013.

[55] L. Ghiani, V. Mura, S. Tocco, G. L. Marcialis, and F. Roli, “Livdet 2013 fingerprint liveness detection competition 2013,” in *Proc. IAPR Int. Conf. on Biometrics (ICB)*, 2013.

[56] D. Yambay, J. S. Doyle, K. W. Bowyer, A. Czajka, and S. Schuckers, “LivDet-Iris 2013 - Iris Liveness Detection Competition 2013,” in *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, 2014.

[57] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, “Direct attacks using fake images in iris verification,” in *Proc. COST 2101 Workshop on Biometrics and Identity Management (BioID)*, ser. Springer LNCS-5372, 2008, pp. 181–190.

[58] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, “Evaluation of direct attacks to fingerprint verification systems,” *Journal of Telecommunication Systems, Special Issue of Biometrics Systems and Applications*, vol. 47, pp. 243–254, 2011.

[59] A. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: a public database and a baseline,” in *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, 2011.

[60] Biometrics Institute, “Biometric Vulnerability Assessment Expert Group,” 2011, (http://www.biometricsinstitute.org/pages/biometric-vulnerabilityassessment-expert-group-bvaeg.html).

[61] NPL, “National Physical Laboratory: Biometrics,” 2010, http://www.npl.co.uk/biometrics.

[62] CESG, “Communications-Electronics Security Group - BiometricWorking Group (BWG),” 2001, (https://www.cesg.gov.uk/policyguidance/biometrics/Pages/index.aspx).

[63] BEAT, “BEAT: Biometrics Evaluation and Testing,” 2012, http://www.beat-eu.org/.

[64] TABULA RASA, “Trusted biometrics under spoofing attacks,” 2010, http://www.tabularasa-euproject.org/.

[65] B. Schneier, “Biometrics: Truths and fictions,” *Crypto-Gram Newsletter*, 1998, available on-line at: https://www.schneier.com/crypto-gram-9808.html#biometrics.

[66] ——, “The uses and abuses of biometrics,” *Communications of the ACM*, vol. 48, p. 136, 1999.

[67] Y. Li, K. Xu, Q. Yan, Y. Li, and R. Deng, “Understanding OSN-based facial disclosure against face authentication systems,” in *Proc. ACM Asia Symposium on Information, Computer and Communications Security (ASIACCS)*, 2014, pp. 413–424.

[68] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio, “An evaluation of direct and indirect attacks using fake fingers generated from ISO templates,” *Pattern Recognition Letters*, vol. 31, pp. 725–732, 2010.

[69] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of artificial gummy fingers on fingerprint systems,” in *Proc. SPIE Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, 2002, pp. 275–289.

[70] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, “A new forgery scenario based on regaining dynamics of signature,” in *Proc. IAPR Int. Conf. on Biometrics (ICB)*. Springer LNCS-4642, 2007, pp. 366–375.

[71] B. Mjaaland, P. Bours, and P. Gligoroski, “Walk the walk: Attacking gait biometrics by imitation,” in *Proc. Int. Conf. on Information Security (ISC)*, ser. Springer LNCS-6531, 2010.

[72] H. Chen, H. Valizadegan, S. Soltysiak, and A. Jain, “Fake hands: spoofing hand geometry systems,” in *Proc. Biometrics Consortium Conference (BCC)*, 2005.

[73] F. Alegre, R. Vipperla, N. Evans, and B. Fauve, “On the vulnerability of automatic speaker recognition to spoofing attacks with artificial signals,” in *Proc. European Signal Processing Conference (EUSIPCO)*, 2012, pp. 36–40.

[74] Q. Bin, P. Jian-Fei, C. Guang-Zhong, and D. Ge-Guo, “The anti-spoofing study of vein identification system,” in *Proc. Int. Conf. on Computational Intelligence and Security (ICCIS)*, 2009, pp. 357–360.

[75] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, “Evaluation of serial and parallel multibiometric systems under spoofing attacks,” in *Proc. IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2012, pp. 283–288.

[76] P. Tome, M. Vanoni, and S. Marcel, “On the vulnerability of finger vein recognition to spoofing,” in *Proc. IEEE Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, 2014.

[77] A. Al-Ajlan, “Survey on fingerprint liveness detection,” in *Int. Workshop on Biometrics and Forensics (IWBF)*, 2013.

[78] C. Sousedik and C. Busch, “Presentation attack detection methods for fingerprint recognition systems: a survey,” *IET Biometrics*, pp. 1–15, 2014.

[79] E. Marasco and A. Ross, “A survey on anti-spoofing schemes for fingerprints,” *ACM Computing Surveys*, vol. 47, pp. 1–36, 2014.

[80] P. Johnson, R. Lazarick, E. Marasco, E. Newton, A. Ross, and S. Schuckers, “Biometric liveness detection: Framework and metrics,” in *Proc. NIST Int. Biometric Performance Conference (IBPC)*, 2012.

[81] R. Lazarick, “Spoofs, subversion and suspicion: Terms and concepts,” in *Proc. NIST Int. Biometric Performance Conference (IBPC)*, 2012.

[82] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer, 2009.

[83] A. M. Namboodiri, S. Saini, X. Lu, and A. K. Jain, “Skilled forgery detection in on-line signatures: a mutimodal approach,” in *Proc. Int. Conf. on Biometric Authentication (ICBA)*, 2004.

[84] J. Fierrez-Aguilar, “Adapted fusion schemes for multimodal biometric authentication,” Ph.D. dissertation, Universidad Politecnica de Madrid, 2006.

[85] R. N. Rodrigues, N. Kamat, and V. Govindaraju, “Evaluation of biometric spoofing in a multimodal system,” in *Proc. IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2010.

[86] P. A. Johnson, B. Tan, and S. Schuckers, “Multimodal fusion vulnerability to non-zero effort (spoof) imposters,” in *Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS)*, 2010.

[87] B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, “Security evaluation of biometric authentication systems under realistic spoofing attacks,” *IET Biometrics*, vol. 1, pp. 11–24, 2012.

[88] Z. Akhtar, M. Rizwan, and S. Kale, “Multimodal biometric fusion: Performance under spoof attacks,” *Journal of Intelligent Systems*, vol. 20, pp. 353–372, 2011. IEEE ACCESS, VOL. XX, NO. XX, MONTH YEAR 20

[89] Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti, “MoBio-LivDet: Mobile biometric liveness detection,” in *Proc. of IEEE Int. Conf. on Advanced Video and Signal-Based Surveillance (AVSS)*, 2014, pp. 187–192.

[90] P. Coli, G. L. Marcialis, and F. Roli, “Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device,” *Int. Journal of Image and Graphics*, pp. 495–512, 2008.

[91] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, “Fingerprint image reconstruction from standard templates,” *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, pp. 1489–1503, September 2007.

[92] S. Shah and A. Ross, “Generating synthetic irises by feature agglomeration,” in *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, 2006, pp. 317–320.

[93] J. Galbally, R. Plamondon, J. Fierrez, and J. Ortega-Garcia, “Synthetic on-line signature generation. Part I: Methodology and algorithms,” *Pattern Recognition*, vol. 45, pp. 2610–2621, 2012.

[94] IBG, “Biometrics market and industry report 2009-2014,” International Biometric Group, Tech. Rep., 2008.

[95] B. Gipp, J. Beel, and I. Rssling, *ePassport: The World’s New Electronic Passport*. Scotts Valley, CA: CreateSpace, 2007.

[96] Ministerio del Interior, Gobierno de Espana, “DNI electronico,” 2013, http://www.dnielectronico.es/Asi es el dni electronico/descripcion.html.

[97] G. Aggarwal, S. Biswas, P. J. Flynn, and K. W. Bowyer, “A sparse representation approach to face matching across plastic surgery,” in *Proc. Workshop on the Applications of Computer Vision (WACV)*, 2012, pp. 113–119.

[98] H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, “Recognizing surgically altered face images using multiobjective evolutionary algorithm,” *IEEE Trans. on Information Forensics and Security*, vol. 8, pp. 89–100, 2013.

[99] Y. Sun, M. Tistarelli, and D. Maltoni, “Structural similarity based image quality map for face recognition across plastic surgery,” in *in Proc. IEEE Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 2013.

[100] R. Singh, M. Vatsa, H. S. Bhatt, S. Bharadwaj, A. Noore, and S. S. Nooreyezdan, “Plastic surgery: a new dimension to face recognition,” *IEEE Trans. on Information Forensics and Security*, vol. 5, pp. 441–448, 2010.

[101] A. Dantcheva, C. Chen, and A. Ross, “Can facial cosmetics affect the matching accuracy of face recognition systems?” in *Proc. IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2013, pp. 391–398.

[102] X. Tan, Y. Li, J. Liu, and L. Jiang, “Face liveness detection from a single image with sparse low rank bilinear discriminative model,” in *Proc. European Conference on Computer Vision (ECCV)*, ser. LNCS 6316. Springer, 2010, pp. 504–517.

[103] K. Kollreider, H. Fronthaler, and J. Bigun, “Evaluating liveness by face images and the structure tensor,” in *Proc. IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, 2005, pp. 75–80.

[104] I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” in *Proc. IEEE Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, 2012, pp. 1–7.

[105] Z. Zhiwei, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, “A face antispoofing database with diverse attacks,” in *Proc. IAPR Int. Conf. on Biometrics (ICB)*, 2012, pp. 26–31.

[106] Y. Kim, J. Na, S. Yoon, and J. Yi, “Masked fake face detection using radiance measurements,” *Journal of the Optical Society of America*, vol. 26, pp. 760–766, 2009.

[107] N. Erdogmus and S. Marcel, “Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect,” in *Proc. IEEE Biometrics: Theory, Applications and Systems (BTAS)*, 2013.

[108] N. Kose and J.-L. Dugelay, “On the vulnerability of face recognition systems to spoofing mask attacks,” in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2013.

[109] N. Erdogmus and S. Marcel, “Spoofing face recognition with 3d masks,” *IEEE Transactions on Information Forensics and Security*, vol. 9, pp. 1084–1097, 2014.

[110] ——, “Spoofing 2d face recognition systems with 3d masks,” in *Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, 2013.

[111] B. Peixoto, C. Michelassi, and A. Rocha, “Face liveness detection under bad illumination conditions,” in *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, 2011, p. 35573560.

[112] V. Vijayan, K. W. Bowyer, P. J. Flynn, D. Huang, L. Chen, M. Hansen, O. Ocegueda, S. K. Shah, and I. A. Kakadiaris, “Twins 3D face recognition challenge,” in *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, 2011.

[113] P. J. Phillips, P. J. Flynn, K. W. Bowyer, R. W. V. Bruegge, P. J. Grother, G. W. Quinn, and M. Pruitt, “Distinguishing identical twins by face recognition,” in *Proc. IEEE Int. Conf. on Automatic Face and Gesture Recognition and Workshops (FG)*, 2011, pp. 185–192.

[114] B. Klare, A. A. Paulino, and A. K. Jain, “Analysis of facial features in identical twins,” in *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, 2011.

[115] Z. Sun, A. A. Paulino, J. Feng, Z. Chai, T. Tan, and A. K. Jain, “A study of multibiometric traits of identical twins,” in *Proc. SPIE Biometric Technology for Human Identification (BTHI)*, 2010.

[116] G. Chetty and M. Wagner, “Liveness detection using cross-modal correlations in face-voice person authentication,” in *Proc. Annual Conf. of the International Speech Communication Association (Interspeech)*, 2005, pp. 2181–2184.

[117] C. Sanderson, “The VidTIMIT database,” IDIAP Institute of Research, Tech. Rep., 2002.

[118] G. Chetty and M. Wagner, “UCBN: A new audio-visual broadcast news corpus for multimodal speaker verification studies,” in *Proc. Australian Int. Conf. on Speech Science and Technology (AICST)*, 2005, pp. 281–286.

[119] K. Kollreider, H. Fronthaler, and J. Bigun, “Verifying liveness by multiple experts in face biometrics,” in *Proc. IEEE Int. Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2008.

[120] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, “Face liveness detection by learning multispectral reflectance distributions,” in *Proc. IEEE Int. Conf. on Automatic Face and Gesture Recognition (AFGR)*, 2011, pp. 436–441.

[121] N. Kose and J.-L. Dugelay, “Reflectance analysis based countermeasure technique to detect face mask attacks,” in *Proc. IEEE Int. Conf. on Digital Signal Processing (DSP)*, 2013.

[122] T. I. Dhamecha, A. Nigam, R. Singh, and M. Vatsa, “Disguise detection and face recognition in visible and thermal spectrums,” in *Proc. IEEE Int. Conf. on Biometrics (ICB)*, 2013.

[123] G. Pan, L. Sun, Z. Wu, and S. Lao, “Eyeblink-based anti-spoofing in face recognition from a generic webcamera,” in *Proc. IEEE Int. Conf. on Computer Vision (ICCV)*, 2007, pp. 14–20.

[124] M. de Marsico, M. Nappi, D. Riccio, and J.-L. Dugelay, “Moving face spoofing detection via 3d projective invariants,” in *Proc. IEEE Int. Conf on Biometrics (ICB)*, 2012.

[125] T. de Freitas Pereira, A. Anjos, J. M. de Martino, and S. Marcel, “LBP-TOP based countermeasure against facial spoofing attacks,” in *Int. Workshop on Computer Vision with Local Binary Pattern Variants (ACCV)*, 2012.

[126] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, “Computationally efficient face spofing detection with motion magnfication,” in *Proc. IEEE Int. Conf. on Computer Vision and Pattern Recognition Workshops (CVPR-W)*, 2013, pp. 105–110.

[127] J. Maatta, A. Hadid, and M. Pietikainen, “Face spoofing detection from single images using texture and local shape analysis,” *IET Biometrics*, vol. 1, pp. 3–10, 2012.

[128] J. Komulainen, A. Hadid, and M. Pietikainen, “Context based face anti-spoofing,” in *Proc. IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2013.

[129] I. Pavlidis and P. Symosek, “The imaging issue in an automatic face/disguise detection system,” in *Proc. IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications*, 2000, pp. 15–24.

[130] H. K. Jee, S. U. Jung, and J. H. Yoo, “Livenes detection for embedded face recognition system,” *Int. Journal of Biological and Life Sciences*, vol. 1, pp. 235–238, 2005. IEEE ACCESS.

[131] J.-W. Li, “Eye blink detection based on multiple gabor response waves,” in *Proc. IEEE Int. Conf. on Machine Learning and Cybernetics (ICMLC)*, 2008, p. 28522856.

[132] L. Wang, X. Ding, and C. Fang, “Face live detection method based on physiological motion analysis,” *Tsinghua Science Technology*, vol. 14, pp. 685–690, 2009.

[133] J. Bigun, H. Fronthaler, and K. Kollreider, “Assuring liveness in biometric identity authentication by real-time face tracking,” in *Proc. IEEE Int. Conf. on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS)*, 2004, pp. 104–112.

[134] A. Ali and F. D. D. Hoque, “Liveness detection using gaze collinearity,” in *Proc. IEEE Int. Conf. on Emerging Security Technologies (ICEST)*, 2012, pp. 62–65.

[135] W. Bao, H. Li, N. Li, and W. Jiang, “A liveness detection method for face recognition based on optical flow field,” in *Proc. Int. Conf. on Image Analysis and Signal Processing (ICIASP)*, 2009, pp. 233–236.

[136] A. Anjos, M. M. Chakka, and S. Marcel, “Motion-based counter-measures to photo attacks in face recognition,” *IET Biometrics*, 2013, in press.

[137] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, “Face liveness detection using 3d structure recovered from a single camera,” in *Proc. IEEE/IAPR Int. Conf. on Biometrics (ICB)*, 2013.

[138] Y. Kim, J. H. Yoo, and K. Choi, “A motion and similarity-based fake detection method for biometric face recognition systems,” in *Proc. IEEE Int. Conf. on Consumer Electronics (ICCE)*, 2011, pp. 171–172.

[139] G. Pan, L. Sun, Z. Wu, and Y. Wang, “Monocular camera-based face liveness detection by combining eyeblink and scene context,” *Telecommunication Systems*, vol. 47, pp. 215–225, 2011.

[140] J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Z. Li, “Face liveness detection by exploring multiple scenic clues,” in *Proc. Int. Conf. on Control, Automation, Robotics and Vision (ICARCV)*, 2012.

[141] A. da Silva Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, “Face spoofing detection through partial least squares and low-level descriptors,” in *Proc. Conf. on Graphics, Patterns and Images (SIBGRAPI)*, 2012.

[142] J. Komulainen, A. Hadid, and M. Pietikainen, “Face spoofing detection using dynamic texture,” in *Proc. Assian Conf. on Computer Vision Workshops (ACCV-W)*, ser. Springer LNCS-7728, 2012, pp. 146–157.

[143] J. Li, Y. Wang, T. Tan, and A. K. Jain, “Live face detection based on the analysis of fourier spectra,” in *Proc. SPIE Biometric Technology for Human Identification (BTHI)*, 2004, pp. 296–303.

[144] W. Schwartz, A. Rocha, and H. Pedrini, “Face spoofing detection through partial least squares and low-level descriptors,” in *Proc. IEEE Int. Joint Conference on Biometrics (IJCB)*, 2011.

[145] J. Yang, Z. Lei, S. Liao, and S. Z. Li, “Face liveness detection with component dependent descriptor,” in *Proc. IEEE/IAPR Int. Conf. on Biometrics (ICB)*, 2013.

[146] N. Kose and J.-L. Dugelay, “Classification of captured and recaptured images to detect photograph spoofing,” in *Proc. IEEE Int. Conf on Informatics, Electronics and Vision (ICIEV)*, 2012, pp. 1027–1032.

[147] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, “Is physics-based liveness detection truly possible with a single image?” in *Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS)*, 2010.

[148] J. Maatta, A. Hadid, and M. Pietikainen, “Face spoofing detection from single images using micro-texture analysis,” in *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, 2011, DOI: 10.1109/IJCB.2011.6117510.

[149] S. Kim, S. Y. K. Kim, Y. Ban and S. Lee, “Face liveness detection using variable focusing,” in *Proc. IEEE/IAPR Int. Conf. on Biometrics (ICB)*, 2013.

[150] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J. Kim, “Face liveness detection based on texture and frequency analysis,” in *Proc. IEEE Int. Conf. on Biometrics (ICB)*, 2012, pp. 62–72.

[151] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristri, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Z. Li, W. R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrillon-Santana, J. Maatta, A. Hadid, and M. Pietikainen, “Competition on countermeasures to 2-d facial spoofing attacks,” in *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, 2011.

[152] F. J. Prokoski and R. B. Biel, *Biometrics: personal identification in networked society*. Kluwer, 1999, ch. Infrared identification of faces and body parts, pp. 191–212.

[153] P. Buddharaju, I. Pavlidis, P. Tsiamyrtzis, and M. Bazakos, “Physiology-based face recognition in the thermal infrared spectrum,” *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, pp. 613–626, 2007.

[154] G. Hermosilla, J. R. del Solar, R. Verschae, and M. Correa, “A comparative study of thermal face recognition methods in unconstrained environments,” *Pattern Recognition*, vol. 45, pp. 2445–2459, 2012.

[155] A. Seal, S. Ganguly, D. Bhattacharjee, M. Nasipuri, and D. K. Basu, “Automated thermal face recognition based on minutiae extraction,” *International Journal of Computational Intelligence Studies*, vol. 2, pp. 133–156, 2013.

[156] K. W. Bowyer, K. Chang, and P. Flynn, “A survey of approaches and challenges in 3D and multi-modal 3D + 2D face recognition,” *Computer Vision and Image Understanding*, vol. 101, pp. 1–15, 2006.

[157] N. Kose and J.-L. Dugelay, “Shape and texture based countermeasure to protect face recognition systems against mask attacks,” in *Proc. IEEE Int. Conf. on Computer Vision and Pattern Recognition Workshops (CVPR-W)*, 2013, pp. 11–116.

[158] ——, “Countermeasure for the protection of face recognition systems against mask attacks,” in *Proc. IEEE Int. Conf. on Automatic Face and Gesture Recognition (FG)*, 2013.

[159] L. Sun, W. Huang, and M. Wu, “TIR/VIS correlation for liveness detection in face recognition,” in *Proc. Int. Conf. on Computer Analysis of Images and Pattern (CAIP)*, ser. Springer LNCS-6855, 2011, pp. 114–121.

[160] C. C. Chibelushi, F. Deravi, and J. Mason, “A review of speech-based bimodal recognition,” *IEEE Trans. on Multimedia*, vol. 4, pp. 23–37, 2002.

[161] G. Chetty and M. Wagner, “Liveness verification in audio-video speaker authentication,” in *Proc. of Int. Conf. on Spoken Language Processing (ICSLP)*, 2004, pp. 2509–2512.

[162] E. A. Rua, H. Bredin, C. G. Mateo, and D. G. Jimenez., “Audio-visual speech asynchrony detection using co-inertia analysis and coupled hidden markov models,” *Pattern Analysis and Applications*, vol. 12, pp. 271–284, 2009.

[163] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, “Realtime face detection and motion analysis with application in ”liveness” assessment.” *IEEE Trans. on lnformation Forensics and Security*, vol. 2, pp. 548–558, 2007.

[164] I. Chingovska, A. Anjos, and S. Marcel, “Anti-spoofing in action: joint operation with a verification system,” in *Proc. IEEE Int. Conf. on Computer Vision and Pattern Recognition Workshops (CVPR-W)*, 2013, pp. 98–104.

[165] T. de Freitas Pereira, A. Anjos, J. M. D. Martino, and S. Marcel, “Can face anti-spoofing countermeasures work in a real world scenario?” in *Proc. IEEE Int. Conf. on Biometrics (ICB)*, 2013.

[166] R. Tronci, F. Roli, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, and M. Ristori, “Fusion of multiple clues for photo-attack detection in face recognition systems,” in *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, 2011, pp. 1–6.

[167] J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, and S. Marcel, “Complementary countermeasures for detecting scenic face spoofing attacks,” in *Proc. IEEE/IAPR Int. Conf. on Biometrics (ICB)*, 2013.

[168] T. Hastie, R. Tibshirani, and J. Friedman., *The Elements of Statistical Learning*. Springer-Verlag, 2001.

[169] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli, and S. Schuckers, “First international fingerprint liveness detection competition – livdet 2009,” in *Proc. IAPR Int. Conf. on Image Analysis and Processing (ICIAP)*. Springer LNCS-5716, 2009, pp. 12–23. IEEE ACCESS, VOL. XX, NO. XX, MONTH YEAR 22

[170] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, “LivDet 2011 - fingerprint liveness detection competition 2011,” in *Proc. Int. Joint Conf. on Biometrics (IJCB)*, 2011.

[171] R. Bodade and D. S. Talbar, “Dynamic iris localisation: A novel approach suitable for fake iris detection,” *Int. Journal of Computer Information Systems and Industrial Management Applications*, vol. 2, pp. 163–173, 2010.

[172] H. Zhang, Z. Sun, and T. Tan, “Contact lense detection based on weighted LBP,” in *Proc. IEEE Int. Conf. on Pattern Recognition (ICPR)*, 2010, pp. 4279–4282.

[173] H. Zhang, Z. Sun, T. Tan, and J. Wang, “Learning hierarchical visual codebook for iris liveness detection,” in *Proc. IEEE Int. Joint Conf. on Biometrics (IJCB)*, 2011.

[174] R. Bodade and S. Talbar, “Fake iris detection: A holistic approach,” *International Journal of Computer Applications*, vol. 19, 2011.

[175] A. Mansfield and J. Wayman, “Best practices in testing and reporting performance of biometric devices,” CESG Biometrics Working Group, Tech. Rep., August 2002, (http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf).

[176] A. S. Georghiades, P. N. Belhumeur, and D. J. Kriegman, “From few to many: Illumination cone models for face recognition under variable lighting and pose,” *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 23, pp. 643–660, 2001.

[177] EAB, “iPhone 5S: heralding a paradigm shift?” European Association for Biometrics, Tech. Rep., 2013, available on-line at: http://www.eab.org/.

[178] A. Kerckhoffs, “La cryptographie militaire,” *Journal des sciences militaires*, vol. 9, pp. 5–83, 1883, available on-line at http://www.petitcolas.net/fabien/kerckhoffs/#english.

[179] B. Schneier, *Secrets and lies*. Wiley, 2000.

[180] BWG, “Biometric security concerns, v1.0,” CESG, UK Government, Tech. Rep., 2003.

[181] B. Fernandez-Saavedra, R. Sanchez-Reillo, R. Alonso-Moreno, and C. Sanchez-Avila, “Evaluation methodoloy for fake ssample detection in biometrics,” in *Proc. Int. Carnahan Conf. on Security Technology (ICCST)*, 2008.

[182] E. Marasco, P. Johnson, C. Sansone, and S. Schuckers, “Increase the security of multibiometric systems by incorporating a spoofing detection algorithm in the fusion mechanism,” in *Proc. Int. Workshop on Multiple Classifier Systems (MCS)*, ser. Springer LNCS-6713, 2011, pp. 309–318.

[183] A. R. R. Poh, “Biometric system design under zero and non-zero effort attacks,” in *Proc. IEEE Int. Conf. on Biometrics (ICB)*, 2013.

[184] E. Marasco, Y. Ding, and A. Ross, “Combining match scores with liveness values in a fingerprint verification system,” in *Proc. IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS)*, 2012, pp. 418–425.

[185] J. Galbally, S. Marcel, and J. Fierrez, “Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition,” *IEEE Trans. on Image Processing*, 2014, in press.

[186] A. C. Doyle, *The Return of Sherlock Holmes*. Strand Magazine, 1903, ch. The adventure of the Norwood builder.

[187] H. Cummins, “Counterfeit finger-prints,” *Journal of Criminal Law and Criminology*, vol. 25, pp. 665–671, 1934.

[188] B. Geller, J. Almog, and P. Margot, “Fingerprint forgery - a survey,” *Journal of Forensic Sciences*, vol. 46, pp. 731–733, 2001.

[189] S. Kiltz, M. Hildebrandt, J. Dittmann, C. Vielhauer, and C. Kraetzer, “Printed fingerprints: a framework and first results towards detection of artificially printed latent fingerprints for forensics,” in *Proc. SPIE Image Quality and System Performance VIII (IQSP)*, 2011, p. 78670U.

[190] M. Hildebrandt, S. Kiltz, J. Sturm, J. Dittmann, and C. Vielhauer, “High-resolution printed amino acid traces: a first-feature extraction approach for fingerprint forgery detection,” in *Proc. of SPIE Media Watermarking, Security, and Forensics (MWSF)*, 2012, p. 83030J.

[191] M. Hildebrandt, S. Kiltz, and J. Dittmann, “Printed fingerprints at crime scenes: a faster detection of malicious traces using scans of confocal microscopes,” in *Proc. SPIE Media Watermarking, Security, and Forensics (MWSF)*, 2013, p. 866509.

[192] S. S. Arora, K. Cao, A. K. Jain, and N. G. Paulter, “3d fingerprint phantoms,” in *Proc. IEEE Int. Conf. on Pattern Recognition (ICPR)*, 2014.

[193] M. F. Barnsley, *Fractals everywhere*. Morgan Kaufmann, 1993, ch. Metric spaces; Equivalent spaces; Classification of subsets; and the space of fractals, pp. 5–41.

[194] J. Henrikson, “Completeness and total boundedness of the hausdorff metric,” *MIT Undergraduate Journal of Mathematics*, pp. 69–80, 1999.

[195] D. Huttenlocher and W. Rucklidge, “A multiresolution technique for comparing images using the hausdorff distance,” Cornell University, Department of Computer Science, Tech. Rep. Technical Report 1321, 1992.

[196] P. Cignoni, C. Rocchini, and R. Scopigno, “Metro: Measuring error on simplified surfaces,” *Computer Graphics Forum*, vol. 17, pp. 164–174, 1998.

[197] Y. Wang and C.-S. Chua, “Robust face recognition from 2D and 3D images using structural hausdorff distance,” *Image and Vision Computing*, vol. 24, pp. 176–185, 2006.

[198] ArtecID. (2014) Artecid - ARTEC 3D face logon: Data sheet. http://www.artecid.com/resources.html. ArtecID. [Online].

[199] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, “Overview of the face recognition grand challenge,” in *Proc. IEEE Int. Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2005, pp. 947–954.

[200] A. Kerckhoffs, “La cryptographie militaire,” *Journal des sciences militaires*, vol. 9, pp. 5–83, 1883, available on-line at http://www.petitcolas.net/fabien/kerckhoffs/#english.

European Commission
EUR 27053 EN – Joint Research Centre – Institute for Protection and Security of the citizen

Title: Biometric Spoofing: A JRC Case Study in 3D Face Recognition

Author(s): Javier Galbally, Riccardo Satta, Monica Gemo, Laurent Beslay

Luxembourg: Publications Office of the European Union

2014 – 65 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-45024-2
doi: 10.2788/00790

LB-NA-27053-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

doi: 10.2788/00790

ISBN 978-92-79-45024-2